(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105264817 B
(45)授权公告日 2019.06.04

(21)申请号 201480025044.8

(22)申请日 2014.03.13

(65)同一申请的已公布的文献号
申请公布号 CN 105264817 A

(43)申请公布日 2016.01.20

(30)优先权数据
13/800,641 2013.03.13 US

(85)PCT国际申请进入国家阶段日
2015.11.03

(86)PCT国际申请的申请数据
PCT/FI2014/050184 2014.03.13

(87)PCT国际申请的公布数据
WO2014/140426 EN 2014.09.18

(73)专利权人 布科特有限公司
地址 芬兰赫尔辛基

(72)发明人 尤卡·萨洛宁

(74)专利代理机构 北京市浩天知识产权代理事务所(普通合伙) 11276
代理人 宋菲 刘云贵

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/40(2006.01)
G06Q 20/40(2006.01)

(56)对比文件
US 2012310743 A1,2012.12.06,
WO 2012131899 A1,2012.10.04,

审查员 辛海明

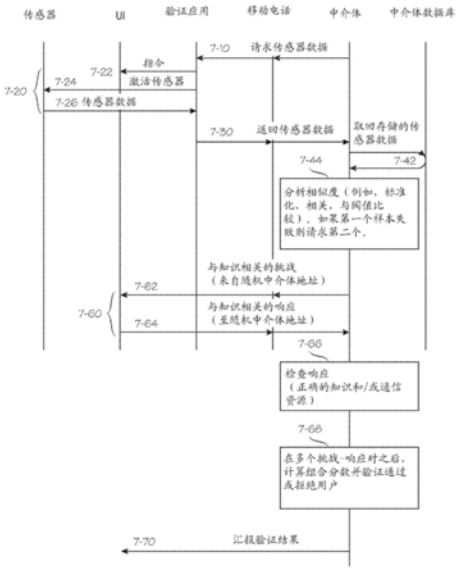
权利要求书4页 说明书14页 附图8页

(54)发明名称

多因素验证技术

(57)摘要

本发明公开了一种验证技术,具有教导阶段和验证阶段。在所述验证阶段中,针对用户收集至少两个类别的验证信息,其中一个类别与用户的可测量物理特征相关,另一个类别与用户可以获得的通信资源相关,第三类别与用户拥有的知识相关。在验证阶段(7-10……7-44),使用收集到的验证信息中的一些信息来形成挑战(7-10……7-24;7-62)以呈现给用户。针对所形成的挑战的响应从用户被接收到,并且至少部分基于与所收集的验证信息的至少一部分的比较(7-44,7-66)来确定接收到的响应的正确性。针对该响应计算正确性指标。如果正确性指标满足或超过第一阈值,则该用户验证通过。



CN 105264817 B

1.一种数据处理系统(1-100,1-300,3-100,1-620,MT),包括:

-存储器系统(3-150),存储程序代码指令(3-160)和数据(3-180);

-处理系统(3-110),包括至少一个处理单元(CP1……CPn),其中所述处理系统执行所述程序代码指令的至少一部分并处理所述数据;

其中,所述存储器系统包括通过所述处理系统可执行的至少一个验证元件,其中,所述至少一个验证元件指示所述处理系统:

-执行与至少一个用户(1-600)相关的至少一个教导阶段(5-22……5-40),其中,在所述至少一个教导阶段中,针对所述用户收集如下至少三个类别中至少两个类别的验证信息:

-第一类别(6-20),关于所述用户的可测量物理特征,所述用户的可测量物理特征至少包括用于用户执行至少一个物理姿势的图像的图像数据;

-第二类别,关于由与所述用户相关联的移动设备提供的通信资源(7-60);以及

-第三类别(6-20,7-60),关于所述用户拥有的知识(1-612),

-执行与所述至少一个用户相关的至少一个验证阶段(7-10……7-44),其中收集的验证信息的所述至少两个类别至少包括所述第一类别,

-其中,在所述至少一个验证阶段中,所收集的验证信息的至少一部分用来形成至少一个挑战(7-10……7-24;7-62)以呈现给所述用户,其中,所形成的至少一个挑战包括来自所述第二类别和来自其余两个类别中的至少一个的验证信息,其中所述所形成的至少一个挑战包括作为来自所述第二类别的验证信息的随机生成的地址,所述随机生成的地址必须用于发送至少一个响应从而成为正确的响应,

-其中,针对所形成的挑战的至少一个响应(7-30;7-64)从所述用户被接收到,并且至少部分基于与所收集的验证信息的至少一部分的比较(7-44,7-66)来确定接收到的响应的正确性,

-其中,针对从所述用户接收到的至少一个响应计算至少一个正确性指标;以及

-其中,如果至少一个计算出的正确性指标满足或超过第一阈值,则所述用户验证通过。

2.根据权利要求1所述的数据处理系统,其中,所述用户(1-600)是身份待被所述数据处理系统(1-300,3-100)验证的验证对象。

3.根据权利要求1或2所述的数据处理系统,其中,所述至少一个验证元件部分地在多个用户可以访问的服务器(1-300,3-100)以及与待被验证的所述用户相关联的至少一个通信终端(1-620,MT)上实施。

4.根据权利要求1或2所述的数据处理系统,其中,所述至少一个验证元件在与待被验证的所述用户相关联的通信终端(1-620,MT)中操作。

5.根据权利要求1或2所述的数据处理系统,其中,所述用户与具有至少一个网络地址的通信终端(1-620,MT)相关联。

6.根据权利要求1或2所述的数据处理系统,其中,所述处理系统包括可被多个用户通过各自的通信终端(1-620,MT)访问的至少一个服务器(1-300,3-100),并且所述至少一个验证元件在所述至少一个服务器中操作。

7.根据权利要求1或2所述的数据处理系统,其中,所述第一阈值基于所述用户的身份

待被验证的交易的值和/或特性。

8.根据权利要求1或2所述的数据处理系统，其中，所述第一阈值基于所述用户的先前历史。

9.根据权利要求1或2所述的数据处理系统，其中，所述至少一个验证元件指示所述处理系统：

-在至少一个教导阶段，针对所述用户收集所述至少三个类别中的三个类别的验证信息；以及

-在至少一个验证阶段中，使用收集到的至少三个类别中三个类别的验证信息。

10.根据权利要求9所述的数据处理系统，其中，如果交易的值和/或特性满足一组预定标准，则所述至少一个验证元件指示所述处理系统收集并使用所述至少三个类别中的至少三个类别的验证信息。

11.根据权利要求1或2所述的数据处理系统，其中，所述至少一个验证元件指示所述处理系统随机选择至少一个类别或者在至少验证阶段待使用的类别内的验证信息。

12.根据权利要求1或2所述的数据处理系统，其中，所述第一类别的验证消息包括生理信息和声音特征中的至少一个。

13.根据权利要求12所述的数据处理系统，其中，所述生理信息包括通过与所述用户相关联的通信终端捕获的至少图像数据。

14.根据权利要求13所述的数据处理系统，其中，所述声音特征包括通过与所述用户相关联的通信终端捕获的至少一个声音记录。

15.根据权利要求12所述的数据处理系统，其中，所述生理信息包括与如下特征中的至少一个相关联的图像数据：

-用户的脸部；

-用户的虹膜；

-用户的至少一个指纹。

16.根据权利要求12所述的数据处理系统，其中，所述至少一个验证元件被配置为：

-收集所述图像数据的生理信息的多个数据集；

-随机选择所述多个数据集中的至少一个；

-挑战用户使其通过捕获的对应于所选的至少一个数据集的图像数据做出响应。

17.根据权利要求1或2所述的数据处理系统，其中，所述第二类别的验证信息包括如下信息中的至少一种：

-至少一个蜂窝网络地址；

-使用至少一个蜂窝网络地址的多个不同通信通道；

-至少一个电子邮件地址；以及

-至少一个社交网络地址。

18.根据权利要求17所述的数据处理系统，其中，所述第二类别的验证信息包括多个数据集，其中所述至少一个验证元件被配置为随机选择所述多个数据集中的至少一个。

19.根据权利要求1或2所述的数据处理系统，其中，所述第三类别的验证信息包括如下信息中的至少一个：

-用户名/密码/PIN码；

-真实问题/答案;

-用户的位置;以及

-定时信息。

20.根据权利要求1或2所述的数据处理系统,其中,所述第三类别的验证信息包括多个数据集,并且所述至少一个验证元件被配置为随机选择所述多个数据集中的至少一个。

21.根据权利要求1或2所述的数据处理系统,其中,所述用户身份的验证仅针对特定地点和/或时间是有效的。

22.根据权利要求1或2所述的数据处理系统,其中,所述至少一个验证元件指示所述处理系统:

-在至少一个教导阶段,将至少一条验证信息与紧急情况的指示相关联;以及

-在至少一个验证阶段,通过向至少一个权利机构通知所述紧急情况而对检测到紧急情况的指示做出响应。

23.根据权利要求1或2所述的数据处理系统,其中,所述第三类别的验证信息包括通过与所述用户相关联的通信终端的一个或多个动作传感器捕获的节奏。

24.一种数据处理方法,包括:

-将程序代码指令和数据存储在存储器系统中;

-执行所述程序代码指令的至少一部分,并通过包括至少一个处理单元的处理系统来处理所述数据中的至少一部分;

其中,所述执行指示所述处理系统:

-执行与至少一个用户相关的至少一个教导阶段,其中,在所述至少一个教导阶段中,针对所述用户收集如下至少三个类别中至少两个类别的验证信息:

-第一类别,关于所述用户的可测量物理特征,所述用户的可测量物理特征至少包括用于用户执行至少一个物理姿势的图像的图像数据;

-第二类别,关于由与所述用户相关联的移动设备提供的通信资源;以及

-第三类别,关于所述用户拥有的知识,

-执行与所述至少一个用户相关的至少一个验证阶段,其中收集的验证信息的所述至少两个类别至少包括所述第一类别,

-其中,在所述至少一个验证阶段中,所收集的验证信息的至少一部分用来形成至少一个挑战以呈现给所述用户,其中,所形成的至少一个挑战包括来自所述第二类别和来自其余两个类别中的至少一个的验证信息,其中所述所形成的至少一个挑战包括作为来自所述第二类别的验证信息的随机生成的地址,所述随机生成的地址必须用于发送至少一个响应从而成为正确的响应,

-其中,针对所形成的挑战的至少一个响应从所述用户被接收到,并且至少部分基于与所收集的验证信息的至少一部分的比较来确定接收到的响应的正确性,

-其中,针对从所述用户接收到的至少一个响应计算至少一个正确性指标;以及

-其中,如果至少一个计算出的正确性指标满足或超过第一阈值,则所述用户验证通过。

25.一种非瞬态存储器装置,包括程序代码指令和数据,其中执行所述程序代码指令的至少一部分并通过包括至少一个处理单元的处理系统处理所述数据的至少一部分指示所

述处理系统：

-执行与至少一个用户相关的至少一个教导阶段，其中，在所述至少一个教导阶段中，针对所述用户收集如下至少三个类别中至少两个类别的验证信息：

-第一类别，关于所述用户的可测量物理特征，所述用户的可测量物理特征至少包括用于用户执行至少一个物理姿势的图像的图像数据；

-第二类别，关于由与所述用户相关联的移动设备提供的通信资源；以及

-第三类别，关于所述用户拥有的知识，

-执行与所述至少一个用户相关的至少一个验证阶段，其中收集的验证信息的所述至少两个类别至少包括所述第一类别，

-其中，在所述至少一个验证阶段中，所收集的验证信息的至少一部分用来形成至少一个挑战以呈现给所述用户，其中，所形成的至少一个挑战包括来自所述第二类别和来自其余两个类别中的至少一个的验证信息，其中所述所形成的至少一个挑战包括作为来自所述第二类别的验证信息的随机生成的地址，所述随机生成的地址必须用于发送至少一个响应从而成为正确的响应，

-其中，针对所形成的挑战的至少一个响应从所述用户被接收到，并且至少部分基于与所收集的验证信息的至少一部分的比较来确定接收到的响应的正确性，

-其中，针对从所述用户接收到的至少一个响应计算至少一个正确性指标；以及

-其中，如果至少一个计算出的正确性指标满足或超过第一阈值，则所述用户验证通过。

多因素验证技术

[0001] 专利案件信息

[0002] 本发明要求于2013年3月13日提交的、名称为“多因素验证技术”的美国专利申请序列号13/800,641的优先权。以上指出的母案申请的内容通过引用的方式合并于此。

技术领域

[0003] 本发明涉及电信系统中的验证。可以执行验证来检验用户的身份，并且可选地可以检验诸如地址之类的其他参数。

背景技术

[0004] 已经开发出了若干验证方案来验证数据处理设备或通信终端的用户。一种已知的验证方案涉及教导阶段中，在该阶段，建立新的用户账户包括教导给验证元素的用户名(登录名)和密码。随后的验证阶段包括请求用户输入用户名-密码组合。如果输入的用户名-密码组合与预先存储的(教导过的)组合匹配，则用户的验证结果为肯定的。

[0005] 如此简单的系统很容易受到入侵和欺诈行为的攻击。入侵者可以以多种方式接入验证系统。他们可能会导致在用户的计算机中安装恶意软件。该恶意软件会记录登录期间用户进行的键盘输入并将键盘输入转发给入侵者。另一种技术是窃听验证服务器和用户终端之间的通信通道。第三种技术是侵入验证服务器。

[0006] 已经进行了许多尝试来缓解与当前验证方案相关的安全性问题。许多改进的验证方案是基于被称为“你知道什么，你有什么”的范例(paradigm)。用户名-密码组合是“你知道什么”的实例，而移动网络标识是“你有什么”的实例。例如，验证的教导阶段可能涉及教导用于验证系统的移动标识(例如MSISDN号)。在验证阶段，验证服务器可以生成伪随机码，将该伪随机码发送到用户的移动终端并请求用户在相对短的时间内返回来自另一个终端(例如计算机)的伪随机码。因为现代移动通信系统使用基于PIN码的验证，因而拥有耦合至教导给验证系统的移动标识的移动终端是与被正在被验证的用户相关的安全性的附加度量。参考文件#1和#2(它们是被共同拥有的PCT申请和美国专利申请)分别公开了各种验证技术。特别地，参考文件#1中公开了一种被称为动态对话矩阵(DDM)的技术，在该技术中，中介体(代理服务器)改变分配给短消息服务(SMS)消息的发送方号码并将不同的发送方号码分配给序列中的每个SMS消息。当客户(移动用户)响应该序列中的SMS消息时，每个应答消息具有唯一的发送方地址(移动终端号码)和接收方地址(分配给查询消息的以中介体作为发送方地址的地址)的组合。该发送方地址和接收方地址的唯一组合用作数据结构(称为DDM)的行和列地址，并且由这两个地址标识的单元包含该应答。通过DDM，中介体不仅知道哪个应答属于哪个查询，而且中介体还以一定的合理性知道发送应答消息的移动用户就是查询消息被发送给的个人。没有其他人知道哪个发送方地址已经被分配给感兴趣的查询。因此，没有其他人知道应答消息应当被发送给哪个接收方地址。

[0007] 在参考文件#2中，图9A、图9B和图9B及其相关描述公开了如下技术：其中通用计算机和移动终端的组合被用于验证(以及用于附加功能，这些功能中的一些功能可能与本发

明不相关)。参考文件#2的图10及其相关描述公开了一种系统架构,该系统架构可以用来实现本发明。上述参考文件的内容通过引用的方式并入本文。

[0008] 虽然已知的验证方案已经进行了改进,然而仍然存在一些遗留问题。例如,大多数的验证方案都具有刚性,而这是不必要的,因为这意味着不管交易的值或者用户的先前历史或其他相关因素是什么,都要求相同的安全等级。另一个问题是,用户名、密码和移动标识的组合可能被从一个合法用户盗取。

[0009] 因此,仍然需要对验证技术关于灵活性、安全性或者这二者进行改进。

发明内容

[0010] 本发明的方案是数据处理系统,包括:存储器系统,存储程序代码指令和数据;以及处理系统,包括至少一个处理单元,其中所述处理系统执行所述程序代码指令的至少一部分并处理所述数据。所述存储器系统包括通过所述处理系统可执行的至少一个验证元件。所述至少一个验证元件指示所述处理系统:执行与至少一个用户相关的至少一个教导阶段,其中,在所述至少一个教导阶段中,针对所述用户收集如下至少三个类别中至少两个类别的验证信息:第一类别,关于所述用户的可测量物理特征;第二类别,关于所述用户可以获得的通信资源;以及第三类别,关于所述用户拥有的知识。

[0011] 所述至少一个验证元件还指示所述处理系统执行与至少一个用户相关的至少一个验证阶段。在所述至少一个验证阶段中,所收集的验证信息的至少一部分用来形成至少一个挑战以呈现给所述用户。针对所形成的挑战的至少一个响应从所述用户被接收到,并且至少部分基于与所收集的验证信息的至少一部分的比较来确定接收到的响应的正确性。针对从所述用户接收到的至少一个响应计算至少一个正确性指标;如果至少一个计算出的正确性指标满足或超过第一阈值,则所述用户验证通过。

[0012] 在典型的使用情况下,所述用户是身份待被所述数据处理系统验证的验证对象。可选地,所述至少一个验证元件在多个用户可以访问的服务器上实施。可替代地或此外,至少一个验证元件在与待被验证的所述用户相关联的至少一个通信终端上实施。至少部分在与用户相关联的通信终端上实施验证元件的益处在于,验证元件能够访问用户界面和通信终端的传感器。在一个示例性但非限制性示例中,在所述通信终端上实施的验证元件可以请求用户用他们左手或右手的指定手指对准他们的鼻子,此后验证元件捕获执行该要求姿势的用户的照片,然后将该照片与在教导阶段预先存储的照片相比较,或者将捕获的照片发送到外部验证元件(例如服务器)以与预先存储的照片进行比较。为了增加安全性,指定的手指和手可以随机改变。如本公开中所使用的,“随机”是指以验证对象只能猜到但是不确定知道的方式改变验证挑战。换句话说,如果验证对象不知道变化的顺序,则验证挑战的变化是随机的。本领域技术人员将了解,如果验证元件在用户(验证对象)可以访问的通信终端上部分实施为客户端组件,则该客户端组件必须通过密码技术被保护并且设置有数字认证。

[0013] 所述用户通常与具有至少一个网络地址的通信终端相关联。

[0014] 为了改善灵活性,针对计算出的正确性指标的第一阈值可以基于所述用户的身份待被验证的交易的值和/或特性。例如,对于值较高的交易而言,验证元件可以要求针对计算出的正确性指标的阈值高于值较低的交易。即使在不能确定精确值的情况下,实施验证

方法也是有益的，在验证方法中，访问某些种类或信息(例如医院的病人信息)要求正确性指标的阈值高，即使访问这种信息并没有与之相关的钱数。可替代地或此外，针对计算出的正确性指标的第一阈值可以基于用户的先前历史。

[0015] 为了提供非常高的安全性，在至少一个教导阶段，至少一个验证元件指示处理系统针对所述用户收集至少三个类别的验证信息。在验证阶段，处理系统使用收集到的所述至少三个类别的验证信息。这种非常高的安全性并不是对所有交易而言都是必须的，如果交易的值和/或特性满足预定标准，则验证元件可以指示处理系统收集并使用至少三个类别的验证信息。

[0016] 在使用少于三个类别的信息的情况下，教导阶段可以涉及到收集比在验证阶段使用的更多类别数量的验证信息。换句话说，在验证阶段可以不使用验证信息的一个或两个类别，如果交易的值和/或特性允许这么做的话。在一些实施方式中，验证元件指示处理系统随机选择至少一个类别和/或在至少验证阶段待使用的类别中的验证信息。再次声明，在实践中，“随机”包括“伪随机”，也就是说，验证使用的信息和/或类别以如下方式变化：即，验证对象仅能猜测出在下一个验证阶段将使用哪条验证信息或类别。

[0017] 在一些实施方式中，关于用户的可测量物理特征的所述第一类别的验证消息(即，“你有什么”)包括生理信息和声音特征中的至少一个。这是通过现代智能手机可以测量的用户物理特征的非穷尽列表。例如，可以通过智能手机的摄像头捕获用户脸部、虹膜和/或至少一个指纹的生理信息。可替代地或另外，通过智能手机的麦克风可以捕获用户的声音样本。

[0018] 为了附加的安全性，可以配置验证元件以收集多个可替代的图像数据的生理信息的数据集(“版本”)，其中脸部、虹膜、指纹照片是代表性的示例。然后验证元件可以随机选择多个数据集中的至少一个。例如，该验证元件可以指示用户用他们的左手食指触摸他们的鼻子，或者用他们的右拳头触摸他们的下巴，然后挑战用户使其用捕获到的对应于所选择的一个数据集的图像数据做出响应。换句话说，通过摄像头捕获的随机选择的用户执行姿势的“版本”应当与先前在教导阶段中存储的相同姿势的照片相匹配。

[0019] 第二类别的验证信息(“你有什么”)的实例的示例性但非穷尽列表包括如下信息中的至少一个：至少一个蜂窝网络地址；使用至少一个蜂窝网络地址的多个不同通信通道；至少一个电子邮件地址；以及至少一个社交网络地址。为了提供附加的验证安全性，第二类别的验证信息可以包括多个数据集，该验证元件可以被配置为随机选择多个数据集中的至少一个。例如，验证元件可以指示用户或他们的通信终端发送响应至随机的网络地址/链接。可替代地或另外，验证元件可以指示用户或他们的通信终端在随机选择的网络资源上发送验证信息，该随机选择的网络资源可以是MAC地址，ISDN号等。

[0020] 第三类别的验证信息(“你有什么”)实例的示例性但非穷尽列表包括如下信息中的至少一个：用户名/密码/PIN码；真实问题/答案；用户的位置(例如终端指示的位置)；定时信息。

[0021] 在较简单验证方案的背景中，用户名、密码和/或PIN码的组合是已知的，并且它们可以被用于本公开中验证信息的第三类别中作为“你有什么”的示例。类似于“你母亲少女时的名字是什么”之类的真实问题和答案也是熟知的。用户名、密码、PIN码和真实问题的答案共有的特征是它们都是经由终端的键盘或按键(这可以通过触摸敏感显示器实现)输入

的。应当注意的是，现代智能手机通常包括能够用来收集第三类别的验证信息的传感器。例如，可以指示用户敲打他们喜欢的音乐的节奏。该节奏可以通过智能手机的麦克风收集。可替代地，如果智能手机具有陀螺仪(多维度倾斜或加速度传感器)，则用户可以在空气中敲打或摆动智能手机，通过倾斜或加速度传感器可以捕获到该节奏。知道音乐是什么的合法用户可以敲打出该节奏但是窃听者则难以仅从节奏猜出该音乐或者甚至是记住该节奏。这种方式的更简单版本包括指示用户以只有该合法用户知晓的间隔敲打几个节拍。可替代地或另外，可以以指示用户在空气中描绘姿势或书写文字的方式来利用倾斜或加速度传感器。该描绘或书写被倾斜或加速度传感器捕获并与在教导阶段捕获的预先存储的版本比较。

[0022] 再次说明，如果第三类别的验证信息(“你知道什么”)包括多个数据集并且该元件被配置为从多个数据集中随机选择至少一个数据集，则可以提供附加的安全性。例如，该验证元件可以提出随机选择的问题，指示用户执行随机选择的动作，该动作通过智能手机的传感器捕获并被与在教导阶段预先存储的版本进行比较，等等。

[0023] 在一些实施方式中，(多个)验证元件被配置为仅针对特定地点和/或时间认为用户身份的验证是有效的。例如，可以授权维修工人在某个时间访问特定场所(premises)。

附图说明

[0024] 图1是可以用来授权移动支付的本发明实施例的框图；

[0025] 图2A和图2B是示出图1所示系统中示例性事件系列的信令图；

[0026] 现在参考图2A，接下来将描述涉及到与个体服务提供方的初始交易的示例性使用情况。

[0027] 图3示出了在之前描述的系统中针对各种信息处理和/或中介体服务器的示例性框图；

[0028] 图4示出了移动终端的示意性框图；

[0029] 图5示出了在验证之前的教导阶段中用户可以如何可选地使用互联网浏览器和移动电话这二者；

[0030] 图6是示出在教导阶段从应用商店下载并安装的验证应用可以如何与中介体前端配合的信令图；

[0031] 图7是示出在验证阶段验证应用可以如何与实际的中介体配合的信令图；以及

[0032] 图8是图5所示场景的变型例，其中，服务提供方组织执行初始注册，将别名标识分配给用户，并且中介体仅知晓该用户的别名标识。

具体实施方式

[0033] 1、可以利用验证的典型场景

[0034] 图1、图2A和图2B示出了可以如何配置本发明的实施例来与其他法律实体配合以形成便于提供服务和支付的复合框架。关于该复合框架的以下描述将说明关于验证的多种观点。观点之一是，现代电子商务涉及多个合作实体，自然也涉及到许多相互验证的问题。另一种要说明的观点是，有许多不同的情况，这些情况对于验证过程的要求是不同的，尤其是关于安全性和便利性的要求，这应当被合适地平衡。还有一种要说明的观点是，虽然涉及

到大量的实体，但是对于集中式验证服务器而言仍然可以对于这些实体中的多个或全部实体执行验证。

[0035] 具体而言，图1、图2A和图2B示出了在复合使用情况下的各种特征，在该情况下，移动用户(也是一个或多个支付卡的所有者)使用至少一个通信终端进行验证并且授权经由支付卡发行方或支付处理器重复进行从用户的信用卡至操作为服务提供方的商家的移动支付。如本文所使用的，移动支付是指一种至少部分在移动网络上作用的支付交易。重复进行的移动支付是发生次数超过一次的移动支付。通常，关于先前交易的信息可以被利用以使得后续交易更方便或有效。如本文所示的这种合理的复合使用说明了如下事实：存在大量的影响验证处理所需的安全等级的变量。

[0036] 图1是可以用于授权移动支付的本发明实施例的框图，而图2A和图2B是示出图1所示系统中一系列事件的信令图。图1示出了一种实施方式，其中，称为中介体1-300的集中式验证服务器位于符合PCI的环境1-100中，其中，“PCI”代表支付卡行业。符合PCI的环境1-100的符合规格由PCI安全标准委员会公布，目前是在地址www.pcisecuritystandards.org上公布。从纯技术的角度而言，根本没有必要实施符合PCI的环境或者在该环境中安装中介体，但是这种实施能够有助于诸如支付处理器和商家之类的其他实体信任中介体1-300。

[0037] 符合PCI的环境1-100中的其他元素包括支付处理器1-200、其相关联的数据库1-202和至少一个商家1-205作为法律实体。数据库1-202存储关于用户和商家的通常的账户和地址信息1-210。虽然存储这种信息被认为是针对审计等进行的较好的业务管理，然而严格来说这对于本实施例而言并不是不可或缺的。

[0038] 一些商家1-250通过符合PCI的环境1-100之外的各线上商店或服务提供方1-400、1-401至1-40n进行操作。当讨论代表性的服务提供方时，通常使用参考标号1-400，而当需要提到个体服务提供方时，可以使用参考标号1-401至1-40n。在符合PCI的环境1-100之外的一个重要因素自然是用户，用户中的典代表性用户用参考标号1-600表示。

[0039] 在该实施例中，用户1-600具有多个角色。首先，用户是支付处理器1-200的客户，并且相应地是一个或多个支付卡的所有者，一个或多个支付卡中的一个用参考标号1-610表示。在参考标号1-610表示支付卡的同时，参考标号1-612表示足以全面标识该支付卡的关于支付卡1-610的信息。换句话说，如果没有额外的验证措施，如在本说明书中提到的那些教导，则关于完整的信息1-612的知识可以使得任何具有该知识的人进行支付(诚信支付或欺诈性支付)，该支付可以对支付卡的所有者1-610进行收费。用户1-600也是移动接入网1-500的用户以及至少一个移动终端1-620的用户。

[0040] 当根据图1的系统投入使用时，下面的假设和条件生效：

[0041] 1、在支付处理器1-200和中介体1-300之间存在初始信任关系。例如，该信任关系可以由处理器1-200和中介体1-300的运营方(作为法律实体)之间签署的法律合同来建立，该法律实体指示处理器1-200和中介体1-300(作为网络节点)相互信任。如本文中所使用的，例如，“初始信任关系”可以意味着，支付处理器1-200已经授权中介体1-300在一组初始限制内处理交易。在系统操作期间，可以增加限制。

[0042] 2、在每个服务提供方1-401到1-40n与支付处理器1-200之间存在初始信任关系。在每个服务提供方1-401到1-40n和中介体1-300之间也可以存在初始信任关系。

[0043] 3、在支付处理器1-200和作为一个活多个支付卡1-610的所有者的用户1-600之间

存在初始信任关系。

[0044] 4、在中介体1-300和作为使用移动终端1-620的移动用户的用户1-600之间存在初始信任关系。

[0045] 然而，该组初始信任关系具有一些空白。首先，在支付处理器1-200工作在符合PCI的环境1-100中的使用情况下，重要的是完整的信用卡信息1-612(也就是足以进行欺诈性购买的信息)不会被传递给符合PCI的环境外部。例如，这意味着，虽然中介体1-300被信任以居间调节服务提供方和移动用户(作为支付卡所有者)之间的支付卡交易，然而该中介体必须能够在没有全面标识用户支付卡的信息的情况下进行操作。此外，一个开放性问题是，是什么将每个用户的支付卡1-610和移动终端1-620联系起来。

[0046] 另一个开放性问题是，各种服务供应方1-401到1-40n、或者提供相互相关业务的服务提供方的子集如何可以被授权以向已经授权来自一个服务提供方的移动交易的用户1-600提供服务。

[0047] 现在参考图2A，接下来将描述涉及与个体服务提供方的初始交易的示例性使用情况。在步骤2-2中，用户1-600注册到处理器1-200的网站。在注册时，用户1-600授权示例性服务提供方1-401提供可能对用户的支付卡1-610进行收费的服务。例如，该注册可以在互联网上通过利用任何具有互联网功能的终端执行。现代智能手机可以用作浏览器或具有互联网功能的终端，但应区分电话功能和浏览器功能。电话功能通常通过利用用户身份模块(SIM)验证，而浏览器功能则通常通过利用用户名/密码组合来单独验证，例如，用户名/密码组合在初始注册期间可以通过向用户的email账户发送确认链接来确认。在一些实施方式中，初始注册2-2可能需要银行验证或一些其他形式的强验证，而随后的使用(如配置改变)可能需要较弱的验证，例如初始注册2-2期间发出的用户ID/密码组合。

[0048] 为了授权重复进行移动支付，用户有效地给出了允许服务提供方1-401通过参考支付卡1-610向用户1-600提供服务的许可。在步骤2-4，处理器1-200存储关于用户1-600给出的许可的信息。例如，处理器1-200可以存储信息元组1-212，该信息元组1-212包括用户的真实身份、移动标识、支付卡号和服务提供方的标识。再次说明，信息元组1-212被认为是为了审计目的而进行的良好的业务管理方式，但严格来说，对于实现支付而言它并不是绝对必要的。

[0049] 在步骤2-6，处理器1-200创建“令牌”1-214，“令牌”1-214向中介体1-300指示该信息的元组1-212已经被建立。为了本实施例的目的，令牌1-214是信息元组1-212的充分标识由用户1-600向服务提供方给出的许可的过滤版本或精简版本。例如，关于用户支付卡的完全标识信息1-612可能没有被传递到符合PCI的环境以外的实体。与完全标识信息1-612不同，令牌1-614仅包含足以标识用户/卡所有者1-600的特定支付卡的信息。在目前的上下文中，这样的信息在附图中被示出为“支付卡REF”，因为这些信息项可以使中介体参考用户/卡所有者1-600的特定支付卡1-610。在所示的实例中，“支付卡REF”信息项可以具有值“VISA_4567”，由此，它标识在当前用户的支付卡中标识特定支付卡而没有全面标识该支付卡。在步骤2-8中，发行方/支付处理器1-200将令牌1-214发送到中介体1-300。在可选步骤2-10中，发行方/支付处理器将令牌发送给服务提供方1-401。

[0050] 在步骤2-20中，服务提供方1-401检测到将服务邀约提供给用户1-600的移动终端1-620的机会。服务提供方1-401有多种方式来检测这种机会。例如，服务提供方1-401可检

测到用户将要请求或已请求来自服务提供方的一些服务，并且该服务提供方可以提供一些相关服务给该用户。可替代地或另外，用户1-600可以导航到服务提供方的网站，并请求关于服务的信息，从而允许将服务邀约发送到用户的移动终端。在步骤2-22中，服务提供方1-401将服务建议发送给中介体1-300。该服务建议2-22包含了在步骤2-6中创建的令牌1-214的标识符。该服务建议2-22还包含关于该邀约的细节，比如提供的是什么服务以及价格是多少等等。在步骤2-24中，中介体1-300重新格式化该邀约并将其转发给用户的移动终端1-620。除了邀约的细节之外，重新格式化后的邀约2-24包含“支付卡REF”信息项，该信息项仅针对用户/卡所有者1-600标识支付卡但是没有全面标识该卡。虽然重新格式化后的邀约2-24被发送到用户的移动终端1-620，但服务提供方1-401并不是必须将移动ID发送到中介体1-300，因为移动ID可以从在步骤2-8中被发送至中介体的令牌1-214中获得。

[0051] 在步骤2-26中，用户1-600从他们的移动终端1-620进行响应。假设使用在本专利说明书中别处描述的DDM技术，例如，用户1-600仅需要发送用于表明“是”的“Y”以及用于表明“否”的任何其他内容(没有包括响应)。类似地，该邀约可包含选择列表(例如A、B、C、D)，用户可以通过回复用于选择A的“A”来选择一个选项。即使多个服务提供方1-401至1-40n各自发送多个邀约，DDM技术仍然能够跟踪来自用户的哪个响应对应于来自哪个服务提供方的哪个服务邀约。在步骤2-28中，中介体1-300利用DDM技术从而识别用户响应的是哪个服务邀约。在可选的步骤2-30和2-32中，中介体1-300可以请求来自发行方/服务提供方1-200的接受，例如这可以执行信用核查。如果信用核查的结果是肯定的，则发行方/服务提供方1-200提供对中介体请求的接受。消息2-30和2-32的交互有两个目的。首先，中介体将关于用户接受的信息传递至发行方/支付处理器1-200以用于收费目的，其次，中介体请求发行方/支付处理器1-200携带与发行方/支付处理器的政策相一致的信用或安全核查。在步骤2-34中，假设核查结果是肯定的，那么中介体1-300将用户的接受转发给服务提供方1-401。

[0052] 在步骤2-36中，中介体、发行方/服务提供方和/或服务提供方可以发送确认给移动用户/卡所有者1-600。严格来讲，该确认被认为是好的方式并且是好的业务管理方式，但是对于提供请求的服务而言该确认并不是不可或缺的。在一些实施方式中，可以以不同的顺序和/或通过不同的实体进行步骤2-30及后续步骤。如从图中可以清楚，在步骤2-34之后，中介体、发行方/服务提供方和/或服务提供方中的每一个都同样清楚地知道一切都已就绪，并且任何实体都可以向用户发送确认。

[0053] 虽然上述步骤2-2到2-34足以就一个移动用户/终端与一个服务提供方建立重复支付，然而仍然希望便于将来自多个相关服务提供方的业务邀约组合起来。例如，假设服务提供方1-401是航空公司。在此假设下，机会检测步骤2-20可以被实施，使得航空公司是符合PCI的环境1-100中的商家1-250的一个实例，该实体通知服务提供方1-401，服务提供方1-401是符合PCI的环境1-100外部的线上商店的实例。

[0054] 现在参考图2B，已经参考图2A描述了步骤2-20至2-34，因而不再重复描述。为了读者方便，在图2B中以缩写图例重复了步骤2-20至2-34。

[0055] 图2B中的第二个主要部分，即步骤2-42至2-56，涉及到令牌创建以重复进行从用户1-600至服务提供方2(1-402)的支付。这些步骤实现的很大程度上与参照图2A描述的用于重复进行从用户1-600至服务提供方1(1-402)的令牌创建(详细内容参见步骤2-2至2-8)类似。然而，实际的实施方式是不同的。在图2B的令牌创建阶段(步骤2-42，.....，步骤2-

56)中，并不是用户1-600发起而是中介体1-300发起。因此，用户不必明确地针对每个服务提供方注册移动支付。另一方面，为用户和服务提供放2创建令牌并没有完全超出用户的控制。在一个优选的实现方式中，要求针对相关服务提供方创建令牌的用户许可，但是给用户带来的不便应当限制到最小。步骤2-42至步骤2-56说明实现这个目的的一种方法。

[0056] 作为步骤2-26的结果，中介体1-300知道用户1-600已经授权对来自服务提供方1(1-401)的服务进行移动支付。中介体1-300现在使用这条信息，并在步骤2-42中提示处理器1-200请求用来创建用于用户1-600和服务提供方2(1-402)这一组合的令牌的许可。在步骤2-44中，处理器1-200请求来自用户1-600的创建里令牌的许可。在步骤2-46中，中介体1-300将该请求转发给用户1-600的移动终端1-620。在本实施例中，用户接受令牌创建，并在步骤2-48中发送肯定响应(例如“Y”)。在步骤2-50中，用户创建令牌的许可传送至处理器1-200，该处理器1-200在步骤2-52中创建用于指示用户许可的记录。在步骤2-54中，支付处理器创建实际的令牌，该令牌在步骤2-56中被发送给中介体。该阶段的最后三个步骤，即步骤2-52至步骤2-56与图2A中第一个令牌被创建的各步骤2-4至步骤2-6类似。

[0057] 与图2A中的步骤2-4至步骤2-6的差别之处在于，在图2B中，是中介体基于用户已经请求了来自服务提供方1的服务(和可接受的收费)这一知识来发起令牌创建处理，针对服务提供方1该中介体意识到了相关的服务提供方。中介体不具有令牌创建处理要求的所有信息，也不需要有。相反，中介体仅需要知道用户1-600和服务提供方2(1-402)这一组合的令牌应当被创建，或者应当从用户请求针对这一创建的许可。用户许可和令牌的其余细节(最明显的是支付卡标识信息1-612)已经被处理器1-200获知。

[0058] 这里还需要注意的是，用户需要验证他/她自己和/或指定哪些来自一个或多个服务提供方的多个同时服务邀约被接受以及哪些被拒绝。可以利用本专利说明书中之前描述的DDM技术来提供验证和/或将用户响应与服务邀约匹配。在一些实施方式中，至少对于金额较低的交易和/或与具有良好历史的用户相关的交易而言，可以省略DDM技术。

[0059] 作为在步骤2-56中通知给中介体的令牌创建过程的结果，现在向服务提供方2(1-402)通知令牌创建。该通知步骤2-58特意留下了关于哪个实体发送该通知的开放性问题。取决于实施方式，可以将该通知从处理器1-200或中介体1-300发送，因为它们都具有相同的可用信息。

[0060] 其中服务提供方2(1-402)发送邀约给用户1-600并且用户接受的步骤2-62至步骤2-76与各步骤2-22至步骤2-34类似，唯一的不同在于服务提供方。在第一种情况下(步骤2-22至步骤2-34)，服务提供方是服务提供方1，而在后一种情况下(步骤2-62至步骤2-76)服务提供方是服务提供方2。

[0061] 中介体1-300驻留在符合PCI的环境内并且符合PCI规范和认证这一事实可以具有各种不同的实现方式。例如，中介体可以被雇员进行了安全清查的法律实体实施和操作。可替代地或另外，中介体或者至少它的一些关键部分可以被深受信任的一方或多方安排或监管，中介体的诚信度通过密码技术(例如数字认证)来检验。可替代地或另外，中介体的一些关键部分可以是以类似于移动SIM卡的方式编码的固件，该SIM卡通过使用挑战-响应机制被验证。包括中介体功能的信任关键部分以及挑战-响应机制的软件可以被编码成固件，中介体(作为代理服务器)可以基于该固件执行。

[0062] 2、示例性硬件平台

[0063] 图3示意性示出了在之前描述的系统中进行的各种信息处理和/或中介服务器的示例性框图。例如，大致由参考标号3-100表示的这样的服务器架构可以用来实现中介体1-300和/或针对发行方/支付处理器和服务提供方的服务器。本文所描述的两个主要功能块是服务器计算机3-100和存储系统3-190。服务器计算机3-100包括大致用参考标号3-110表示的一个或多个中央处理单元CP1...CPn。包括多个处理单元3-110的实施例优选地设置有负荷平衡单元3-115，该负荷平衡单元3-115平衡多个处理单元3-110之间的处理负荷。多个处理单元3-110可被实施为独立的处理器组件或作为在单个部件壳体内的物理处理器核心或虚拟处理器。服务器计算机3-100还包括用于与各种数据网络通信的网络接口3-120，各种数据网络大致通过参考标志DN表示。数据网络DN可以包括局域网(例如以太网络)和/或广域网(例如互联网)。假设服务器计算机3-100用作中介体1-300，则它可以经由数据网络DN与其他服务器配合。参考标号3-125表示移动网络接口，通过该移动网络接口该服务器计算机3-100可与各种接入网AN通信，而该接入网反过来为终端用户或客户使用的移动终端MT服务。

[0064] 本实施例的服务器计算机3-100还可以包括本地用户接口3-140。依赖于实施方式，用户接口3-140可以包括用于本地用户接口的本地输入-输出电路，例如键盘、鼠标和显示器(未示出)。可替代地或另外，服务器计算机3-100的管理可远程实施、通过利用网络接口3-120和提供用户界面的任何具有互联网功能的终端来实施。用户接口的性质取决于使用哪种类型的计算机来实施服务器计算机3-100。如果服务器计算机3-100是专用计算机，则它可以不需要本地用户接口，并且服务器计算机3-100可被远程管理，例如从互联网上的网页浏览器进行管理。这种远程管理可以经由服务器计算机用来进行它自己和客户终端之间的传输的相同网络接口3-120来实现。

[0065] 服务器计算机3-100还包括用于存储程序指令、操作参数以及变量的存储器3-150。参考标号3-160表示适用于服务器计算机3-100的程序。

[0066] 服务器计算机3-100还包括用于各种时钟、中断等的电路，这些电路大致通过参考标号3-130表示。服务器计算机3-100还包括至存储系统3-190的存储接口3-145。当服务器计算机3-100关闭时，存储系统3-190可以存储用于实现处理功能的软件，在上电时，该软件被读入半导体存储器3-150中。存储系统3-190在断电期间也保持操作和变量。在大容量实施方式中(即其中单个服务器计算机3-100经由各移动终端MT为大量用户服务)，存储系统3-190可被用来存储与客户和移动终端MT相关联的动态对话矩阵。各种元件3-110至3-150经由总线3-105互相通信，如本领域技术人员熟知的，总线3-105承载地址信号、数据信号以及控制信号。

[0067] 本发明的技术可以在服务器计算机3-100中实现如下。程序组3-160包括用于指示处理器3-110组执行本发明方法的功能(包括验证)的程序代码指令，并且可选地与其他服务器配合以增强服务提供。

[0068] 图4示出了移动终端的示意性框图。移动终端MT包括具有至少一个中央处理单元的处理系统4-202。该移动终端还包括存储器系统4-250，如本领域技术人员熟知的，存储器系统4-250典型地包括快速易失性存储器和较慢的非易失性存储器的组合。此外，移动终端MT包括或利用用户接口4-210，用户接口4-210包括输入电路4-212和输出电路4-214。输入电路4-212包括移动终端的麦克风和用户输入设备，例如按键和/或触摸屏。输出电路4-214

包括移动终端的显示器和耳机或扬声器。移动终端MT还包括接收/发送电路4-220，接收/发送电路4-220包括传输电路4-222、接收电路4-224和天线4-226。用户身份模块SIM 4-230被验证功能使用以验证移动终端的用户并识别用户对于接入网AN的订购。典型的现代移动终端还包括WLAN(无线局域网络)电路4-234，该电路4-234使得移动终端用作接入到WLAN接入点AP的WLAN客户端。

[0069] 为了支持可安装程序模块，移动终端的存储器4-250通常包括例程，以下载可安装程序模块，并将可安装程序模块存储为存储器4-250中的应用(应用程序)4-260以被中央处理单元CP执行。图4示出了一种布置，其中移动终端被配置为，经由数据网DN、接入网AN、天线4-226以及接收电路4-224，从供应方特定或平台特定应用商店AS下载可安装程序模块。代替经由接入网从应用商店下载软件或者除了经由接入网从应用商店下载软件之外，其他的布置同样可行，例如经由数据网DN将可安装程序模块下载到单独的数据终端(未示出)，可以将可安装程序模块从该单独的数据终端传送至移动终端的WLAN电路4-234，或者可以经由一些其他短程连接，例如蓝牙或通用串行总线(USB，未单独示出)。接入网AN通常是具有宽带能力的移动通信网络，而数据网DN典型地是互联网或者一些执行互联网协议(IP)的封闭子网，通常被称为内联网或者外联网。在这一概括水平上，图4中先前讨论的所有元件都可以是相关领域中使用的传统元件。如下文将更详细描述的，经由接入网络AN和数据网DN可以访问一个或多个外部主机。最后，参考标号4-280表示存储器4-250中用于存储参数和临时变量的区域。

[0070] 除了用户接口4-210之外，移动终端典型地包括用于检测环境变量或参数的可选的传感器4-240。传感器4-240的非穷尽列表包括：摄像头、IR(红外)检测/通信电路、GPS和/或其它位置确定电路、罗盘、陀螺仪(倾斜传感器)、RFID(射频识别)和/或NFC(近场通信)电路等。

[0071] 借助传感器4-240，在移动终端中执行的应用4-260可以收集关于移动终端的环境、周边、位置和/或取向的信息。这种基于传感器的信息被统称感测信息。应用4-260包括用于操作传感器的程序实现功能。根据被执行的应用，移动终端可被设置成响应于用户控制而自发地和/或逐步地收集这种感测信息，使得一种类型的感测信息的检测触发应用4-260以指示移动终端收集进一步的信息、感测或其他信息。通过说明性但非限制性示例，感测信息的主要来源可包括移动终端可以用来确定它邻近感兴趣的对象或已知地点的局部辐射。检测这种局部约束的辐射可以被用来验证用户的位置，即，检验出用户是在其中可以接收到局部约束辐射的位置。例如，局部约束辐射可以随时间变化而改变。在移动终端中操作的验证应用捕获局部约束辐射并存储辐射的相关信息内容这一事实证明，在被捕获的内容被传输的时刻移动终端处于辐射范围内。

[0072] 比如红外、蓝牙或近场通信之类的局部约束辐射的检测可以触发该应用收集来自传感器4-240的与取向相关的感测信息，例如，罗盘指向和/或陀螺仪/倾斜信息以及可选的精确GPS信息。移动终端的位置、取向和关于感兴趣的对象附近的信息可以用作验证的多个方面。例如，由移动终端的摄像头捕获的场景虽然没有绝对的确定性但是仍然可以表明移动终端在可以捕获到该场景的位置处。

[0073] 3、示例性验证技术

[0074] 图1和图2A到图2B及其相关描述阐述了在从建立新账户到相对简单的增量购买的

多种情况下如何要求验证。在前面的实例中，移动终端的用户授权了多个支付，并且自然授权该支付的个人需要被验证。本文所描述的技术也可以在与金融交易不相关的验证处理中使用。例如，在线投票处理是选民需要被验证的情况的示例。

[0075] 图3和图4及其描述示出了适用于实施服务器或中介体以及移动终端的硬件平台。以下的公开内容示出了如何利用移动终端平台来改进已知的验证方案。

[0076] 现在参考图5，将描述示例性教导阶段。图5示出了用户1-600如何在教导阶段可选地同时使用互联网浏览器和移动电话这二者。如前文所述，浏览器功能和电话功能可以在单个物理终端中实现，或在不同的物理终端中实现。使用通用计算机作为浏览器的理由可包括希望使用比电话能够提供的更大的键盘和显示器，或者希望使用耦合至通用计算机的智能卡读取器来进行强验证。

[0077] 步骤5-2至步骤5-16涉及本领域中已知的技术因而仅提供了简略的描述。在步骤5-2中，用户1-600开始用来创建新的用户账户的处理。根据本示例的可选特征，用户1-600与用作中介体1-300前端的服务器通信。作为教导过程的一部分，前端将教导结果存储到中介体可以访问的数据库中。通过使用不同的前端，实际的中介体不需要有教导阶段的负担。用户1-600输入他们的标识信息(如标识该用户以及写该用户的地址所需的全名、地址、电子邮件地址、移动标识等)。为了利用支付卡来实现金融交易，用户通常输入如结合图1和图2A至图2B所述的支付卡细节。在步骤5-4中，前端通常执行关于用户的强验证。例如，银行验证和/或智能卡认证以及PIN签名可以用于这一目的。

[0078] 步骤5-10至步骤5-14涉及将移动标识与新创建的用户账户耦合。在步骤5-10中，中介体前端向浏览器发送挑战字，例如随机字符串。在步骤5-12中，用户将随机字符串复制到移动终端，并在步骤5-14中将其从移动终端发送。现在，中介体前端已经证实步骤5-2中输入的移动标识属于在步骤5-2中发起账户创建的个人。由于移动标识被PIN码执行，因而步骤5-10至步骤5-14有助于加强第一验证过程。

[0079] 在步骤5-16中，从供应方特定或平台特定应用商店下载并安装验证应用程序(“应用”)。例如，前端可以指示用户1-600导航到应用商店下载验证应用程序，或前端可以为此目的向移动终端发送链接。作为又一替代方案，前端可请求应用商店向移动终端发送下载链接。下载和安装应用程序是本领域中已知的技术，因而省略其详细描述。

[0080] 在步骤5-22和步骤5-24中，前端发送很多教导问题给浏览器和/或移动终端。在步骤5-26和步骤5-28中，浏览器和/或移动终端发送针对教导问题的响应。箭头5-40示出了将结果存储在某个长期存储器中。一些教导问题归属于第一类别，第一类别是关于用户的可测量物理特征。安装在移动终端中的验证应用为此目的与前端配合。例如，假设用户眼睛的照片将被用作关于可测量物理特征的第一类别中的项。该前端和验证应用可以以下述方式配合。在本说明书中，假设验证应用是一种“智能”应用，即一种需要来自前端的非常少的详细指令的应用。在一种实施方式中，前端请求验证应用返回用户眼睛的照片。验证应用指示用户将该移动终端的摄像头对准用户的左眼或右眼并激活快门(或者验证应用可以激活自定时功能)。当该照片已经被捕获时，验证应用通过确保存在精确的边缘敏锐度来定位照片内的眼睛，适当地裁剪该照片并且可选地检查照片的质量。可替代地，验证应用可以将拍摄的任何内容发送给前端进行处理和质量确保。针对另一只眼睛可以重复该过程。

[0081] 可以在教导阶段通过移动终端捕获的用户的可测量物理特征的另一个示例是如

通过移动终端的麦克风捕获的用户的声音样本。

[0082] 应当注意的是，单个声音捕获可以提供属于两个类别的信息。例如，如果教导阶段涉及指示用户说出或唱出喜爱的短语或歌曲，则声音特征是可测量的物理特征，而用户的密码短语或歌曲的知识是用户拥有知识的示例。面对说出合法用户喜爱短语或歌曲这一挑战的入侵者将必须知道该短语或歌曲是什么，并且还需要复制该合法用户的声音。

[0083] 图6是信令图，说明从应用商店下载并安装的验证应用如何在教导阶段与中介体前端配合。在图6中，用户的移动终端被划分成四个部分。移动电话是指移动终端的通信能力，验证应用程序是指在图5的步骤5-16中从应用商店下载并安装的应用，UI是指在移动终端的用户界面，通过该用户界面该验证应用可以与用户通信，标记为传感器的部分是指现代智能电话的各种传感器。可在验证中使用的传感器的非穷尽列表包括：摄像头、麦克风、陀螺仪(取向或倾斜传感器)、定位设备、时钟和触摸敏感垫或显示器。

[0084] 在步骤6-10中，中介体前端请求验证应用捕获传感器数据，这是用户的特征和/或用户拥有的知识。如移动终端的摄像头捕获的用户的照片或用户的一部分的照片是体现用户特征的传感器数据的一个示意性示例。由移动终端的陀螺仪(取向或倾斜传感器)捕获的姿势或者由移动终端的麦克风或触摸敏感垫或显示器捕获的节奏是体现用户拥有的知识的传感器数据的示意性示例。说出或唱出用户喜爱的短语或歌曲的挑战是表示用户的可测量声音特征加上合法用户喜爱短语或歌曲的知识的传感器数据的示例。

[0085] 让我们首先假设验证应用被配置为捕获一组用户的照片在步骤6-22中，验证应用发送指令到用户界面，使得用户知道期望他们进行的动作。例如，验证应用可以指示用户用他们的右手捏他们的左耳垂同时以能够通过摄像头捕获姿势的方式将移动终端握持在他们的左手中。在步骤6-24中，验证应用激活移动终端的传感器，其在本例中是指摄像头。在步骤6-26中，验证应用接收传感器数据(在本例中：照片)。步骤6-22到步骤6-26合起来用参考标号6-20来表示。这一系列步骤6-20可通过不同的指令以及可选地通过不同的传感器重复任意次数。例如，当足够数量的用户特征部分(例如虹膜)的照片和姿势(例如通过将用户的食指放在嘴巴前面的安静姿势)已经被摄像头捕获时，则验证应用可以指示用户产生喜欢的音乐的节奏。例如，该节奏可以通过移动终端的麦克风、触摸敏感输入或陀螺仪被捕获。再次说明，控制来自中介体前端而不是来自实际中介体的验证教导阶段的原因在于，希望实际中介体的负担尽可能少。在本文描述的场景中，前端将教导阶段的结果存储在中介体可以访问的数据库中。箭头6-30、6-40分别描绘将传感器数据从验证引用发送至中介体前端以及某个长期存储器的动作。

[0086] 图7是信令图，说明验证应用如何在验证阶段与实际的中介体配合。简言之，验证阶段可以包括中介体引导移动终端中安装的验证引用请求传感器数据的步骤，该传感器数据代表用户的可测量物理特征和/或用户拥有的知识。这些是步骤7-10至步骤7-30，这些步骤与图6中示出的对应步骤非常类似，因而省略了重复描述。步骤6-10至步骤6-30与步骤7-10至步骤7-30之间的区别是，首先，图6和图7分别涉及教导阶段和验证阶段，第二，验证阶段被实际的中介体控制，而教导阶段如图6所示被中介体前端控制以缓解实际中介体的负荷。

[0087] 如在教导阶段所执行的(6-40)，代替将返回的传感器数据存储到数据库，中介体现在从数据库中取回先前存储的传感器数据(步骤7-42)。在步骤7-44中，将在验证步骤中

获得的传感器数据集与先前存储的传感器数据集进行比较。由于传感器数据从来都不是完全精确或可重复的，因而这一分析比用户名和密码的比较更模糊。在比较步骤中执行的典型动作是标准化。例如，可以将传感器数据样本的幅度或数量放大，使得样本的峰值、平均值或均方根(RMS)值获得标准化值。

[0088] 之前描述的图7中的步骤(即步骤7-10至步骤7-44)之前或之后可以是涉及到用户拥有的知识或用户可以获得的通信资源或者这二者的挑战响应循环。参考标号7-60指示这样的挑战-响应对。在该示例中，挑战-响应对7-60通过验证用户拥有的知识以及用户可以获得的通信资源而对验证做出贡献。该场景是基于用户移动电话的至少一个地址已经在教导阶段被教导给中介体数据库这一假设。该至少一个地址可以指示用户的电话号码(MSISDN)、电子邮件地址、社交网络地址等。在步骤7-62中，中介体向用户的移动终端发送基于知识的挑战，例如关于用户的第一个宠物、住房、车、船等的问题。在该示例中，中介体将挑战7-62从随机选择的中介体地址发送。在步骤7-64中，用于通过输入所请求的知识而做出响应，并将该响应发送给随机选择的中介体地址。例如，随机选择的中介体地址可以是移动网络地址空间中的数字，并且媒介可以是移动通信系统中的消息，例如短消息(SMS)、多媒体消息(MMS)等。可替代地，中介体可以发送随机格式化的链接以向用户的电子邮件地址做出响应，该电子邮件地址在教导阶段已经被教导给中介体数据库。实际上，随机地址被中介体合适地管理，但是它们对于用户和入侵者而言表现出随机化。只有已经接入到合法用户的移动终端或电子邮件账户的个人可以发送针对该挑战的响应(任何响应，正确或不正确)。并且只有知道哪个答案在教导阶段被教导给中介体数据库的个人可以发送针对该挑战的正确响应。在步骤7-66中，中介体检查响应7-64的正确性。该正确性检查可以与在响应中提供的消息和/或用来传输该响应的通信资源相关。图7描述了信令图，其中如果挑战-响应对不涉及感测数据的收集，则中介体绕过移动终端中安装的验证应用。在可替代的实施方式中，在所有挑战-响应对中都可以利用验证应用。

[0089] 在步骤7-68中，如果用户已经能够提供针对所有挑战的响应，则中介体完成对该用户的验证。如果一些响应不正确，则中介体可能向该用户授予一些其他尝试。可替代地或另外，在验证中使用的一些挑战-响应对没有刚性的正确或错误响应。特别地，与用户的测得的物理特征或基于传感器的验证相关，在验证阶段提供的响应永远不能匹配在学习阶段提供的响应，并且应当采用相关或其他相似度测量。在一些实施方式中，基于用户的测得的物理特征的验证可以计算出统计性代表度量(例如多个挑战-响应对的中间值、平均值等)，并且如果该统计性达标度量满足给定阈值则肯定地完成用户的验证。

[0090] 在步骤7-70中，中介体将验证的结果汇报给感兴趣的多方，这些感兴趣的多方典型地包括用户和诸如服务提供方之类的其他实体。例如，如果验证的目的是支付验证，则中介体可以通知服务提供方具有给定用户ID的用户已经通过验证。

[0091] 图8是图5中所示场景的变型例，其中业务提供方组织执行初始注册，将别名标识分配给该用户，并且该中介体仅知道该用户的别名标识。在图8中，标记“5-xx”的方法步骤与参照图5描述的步骤类似，因而省略了重复描述。一开始的两个步骤5-2’和5-4’标记有一撇，因为它们与图5中的步骤5-2和5-4的不同之处在于，在图8中，这些步骤被服务提供方或服务提供方的组织执行。换句话说，服务提供方针对该用户创建账户，并执行初始验证。步骤8-6和步骤8-8是新的并且在步骤5中没有相对等的步骤。在可以以任何顺序执行这些步

骤中，服务提供方组织将别名标识分配给该用户，将别名标识发送给中介体前端以及发送给用户的终端。服务提供方组织还例如通过将用户终端链接发送给中介体前端而将用户的终端重新引导至中介体前端。从这个点开始，图8中示出的场景类似于图5中示出的场景。当验证完成时，例如图7中所示的步骤7-70，该中介体将通知感兴趣的多方(例如金融机构)具有给定别名标识的用户已经通过验证。

[0092] 前述验证的描述集中在用户的验证上。代替用户验证或者除了用户验证之外，本公开内容可以用来验证要求用户在的位置或者认为用户在的地方。例如，任务是巡视多个地点的安全警官可以通过利用移动终端的传感器收集的感测数据来证明它们的位置。验证用户的位置基本上与验证用户的身份类似。代替收集代表用户的感测数据，移动终端和安装在该终端中的验证应用可以收集代表位置的感测数据。例如，在特定时间和地点捕获的GPS坐标和/或照片可以用来证实用户在该给定时间在该地点。

[0093] 针对给定验证过程要求的挑战-响应循环的数量通常依赖于多个因素，例如，验证执行的交易相关的值、风险或所要求的机密等级、用户的先前历史、可疑活动(例如短时间内突然从一个国家跑到另一个国家)等。

[0094] 通过实施本说明书的各个方案和特征可以实现非常强的验证。可以实现安全等级从而窃取合法用户网络标识的唯一途径就是通过使得该合法用户与罪犯合作来盗窃该实体用户和通信资源。中介体的一些实施例可以通过实施其中一些基于知识的响应被解读为求助或告警消息的特征来防止这种身份盗窃。如果中介体接收到大量的这种消息(例如一个或两个)，则该中介体可以确定该合法用户已经被拐骗。中介体可以通知警察和/或要求金融机构暂时关闭该用户的账户。

[0095] 前述描述(尤其是与图1、图2A和图2B相关的描述)与集中式中介体为大量服务提供方、支付卡发行方、支付处理器、权利机构等服务的实施方式相关。本领域技术人员将认识到，针对单个实体，例如服务提供方，也可以实施和/或管理中介体功能。无论如何，被配置为多个不同实体服务的集中式中介体相对于其中每个实体管理它们各自的验证方法的分布式实施方式具有多个益处。例如，集中式中介体对于用户而言更方便，因为他们只需要教导一个验证系统。该集中式中介体对于金融机构、服务提供方和/或权利结构而言更方便，因为它们根本不需要维护验证系统。还可以实施混合验证方法，其中用户通过银行卡、芯片卡或其他形式的强验证来向金融机构验证他们自己。作为该首次验证的结果，金融机构可以创建用户账户并同意集中式中介体关于单个交易进行验证。

[0096] 参考文件

[0097] 1.PCT申请公开WO2004/019223

[0098] 2.被共同拥有的美国专利申请序列号13/452,229。

[0099] 参考文件的内容通过引用的方式并入本文。

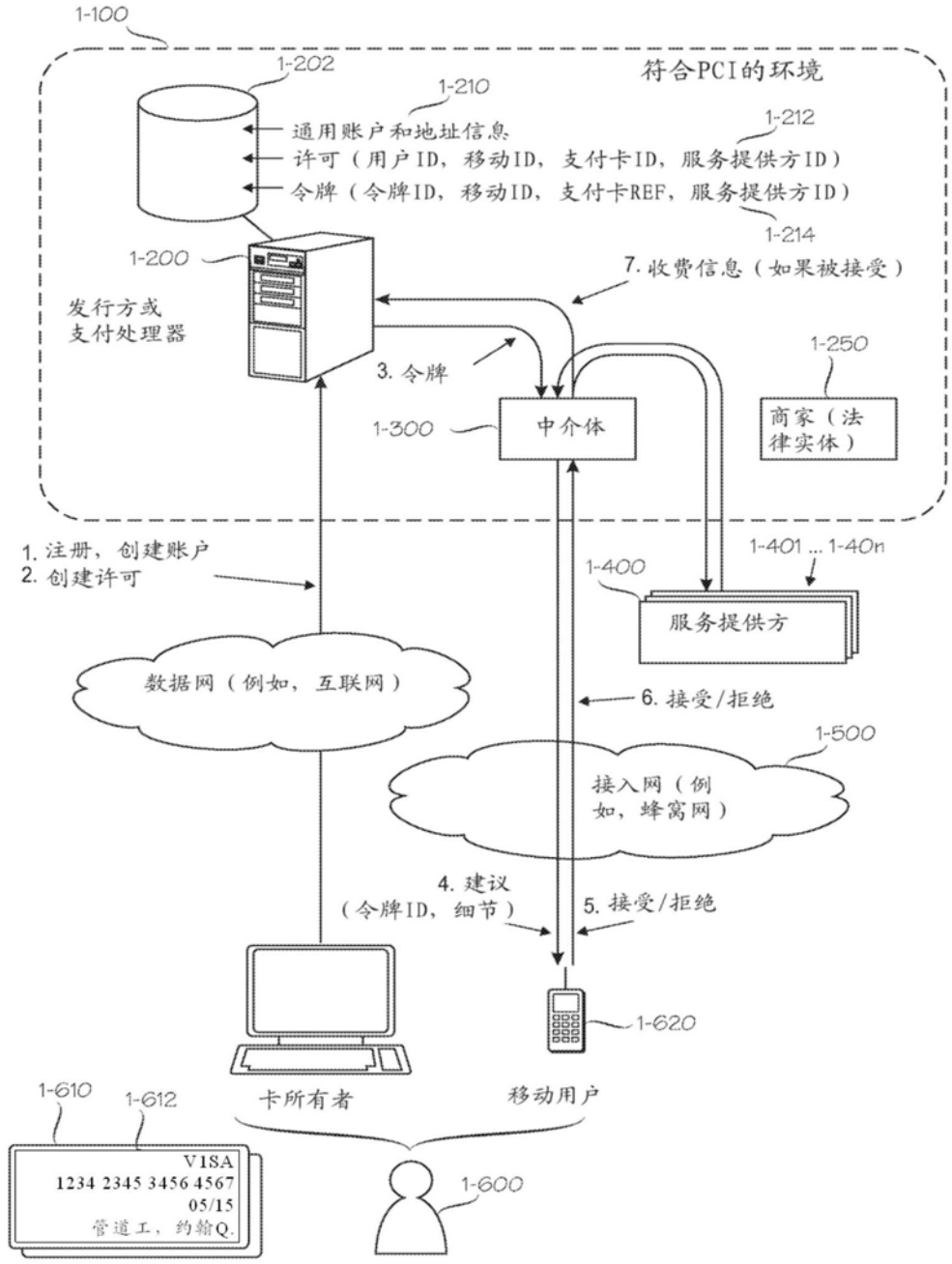

1-100
符合PCI的环境
1-202
1-210
通用账户和地址信息
1-212
许可（用户ID，移动ID，支付卡ID，服务提供方ID）
令牌（令牌ID，移动ID，支付卡REF，服务提供方ID）
1-214
1-200
7. 收费信息（如果被接受）
发行方或
支付处理器
3. 令牌
1-250
1-300
中介体
商家（法律实体）
1. 注册，创建账户
2. 创建许可
1-401 ... 1-40n
1-400
服务提供方
数据网（例如，互联网）
6. 接受/拒绝
1-500
接入网（例如，蜂窝网）
4. 建议
（令牌ID，细节）
5. 接受/拒绝
1-620
1-610
1-612
卡所有者
移动用户
V1SA
1234 2345 3456 4567
05/15
管道工，约翰Q.
1-600

图1

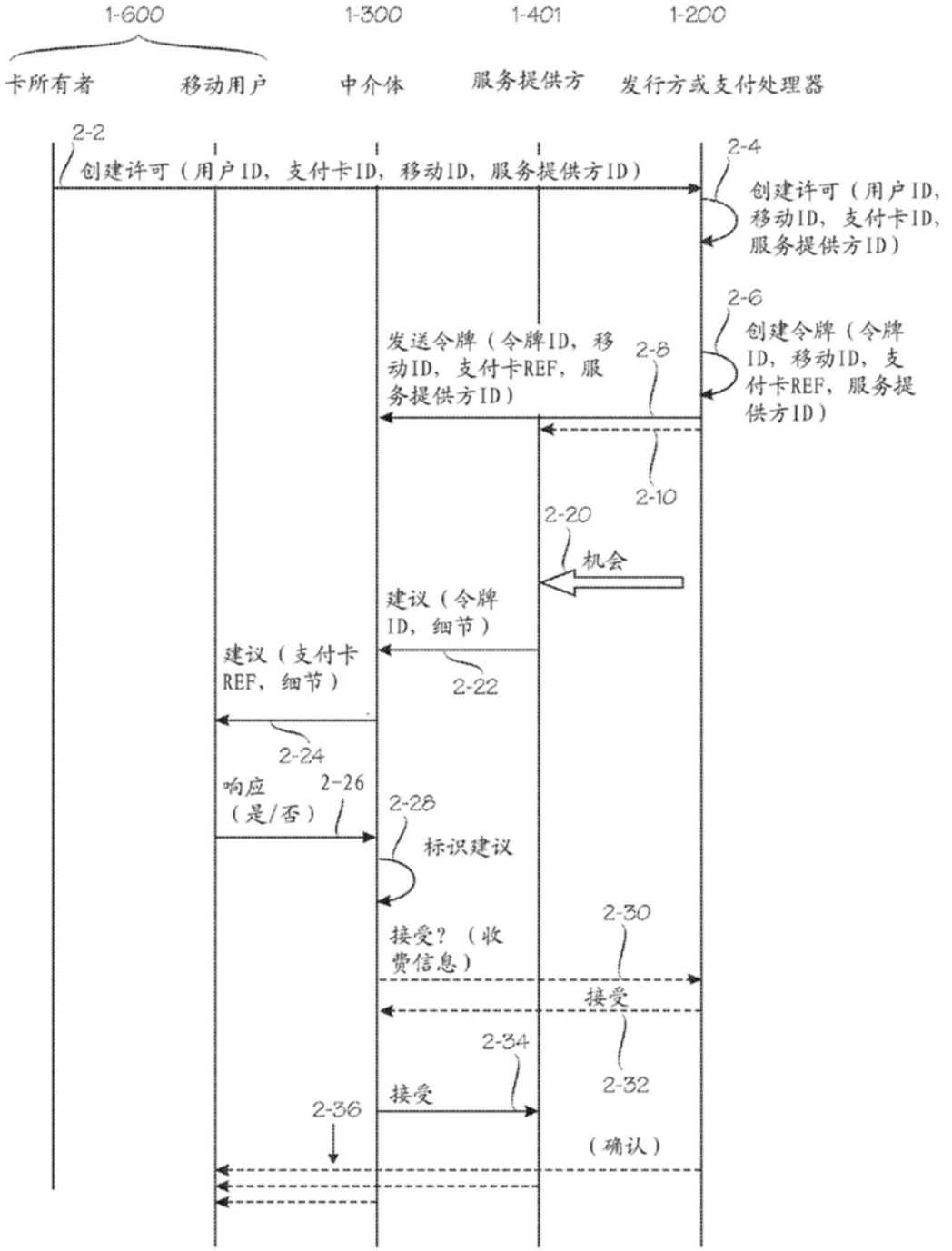

1-600
1-300
1-401
1-200
卡所有者
移动用户
中介体
服务提供方
发行方或支付处理器
2-2
创建许可（用户ID，支付卡ID，移动ID，服务提供方ID）
2-4
创建许可（用户ID，移动ID，支付卡ID，服务提供方ID）
2-6
创建令牌（令牌ID，移动ID，支付卡REF，服务提供方ID）
发送令牌（令牌ID，移动ID，支付卡REF，服务提供方ID）
2-8
2-10
2-20
机会
建议（令牌ID，细节）
建议（支付卡REF，细节）
2-22
2-24
响应（是/否）
2-26
2-28
标识建议
2-30
接受？（收费信息）
接受
2-32
2-34
接受
2-36
（确认）

图2A

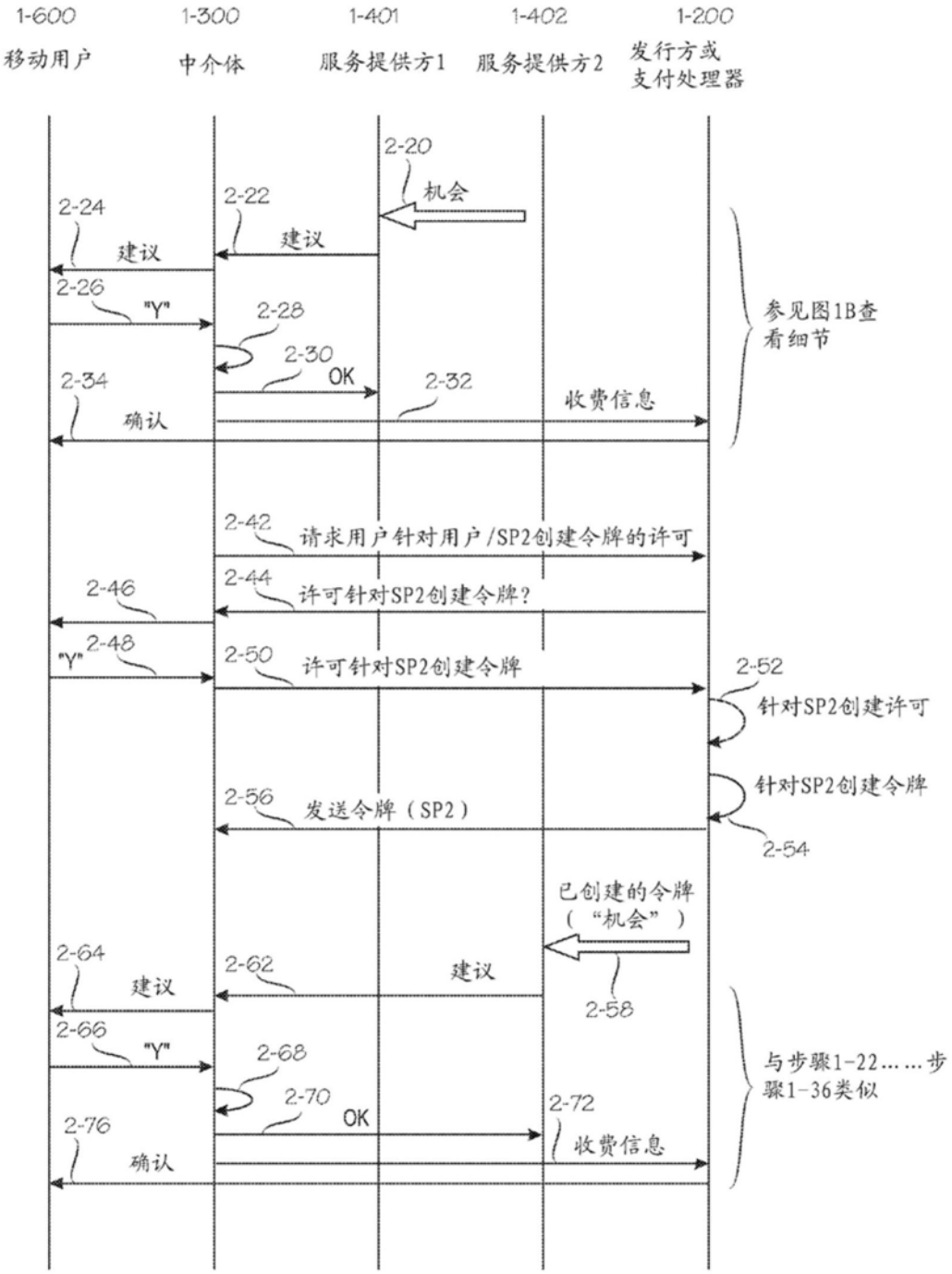

1-600
移动用户
1-300
中介体
1-401
服务提供方1
1-402
服务提供方2
1-200
发行方或
支付处理器
2-20
机会
2-22
建议
2-24
建议
2-26
"Y"
2-28
2-30
OK
2-32
收费信息
2-34
确认
参见图1B查
看细节
2-42
请求用户针对用户/SP2创建令牌的许可
2-44
许可针对SP2创建令牌?
2-46
"Y"
2-48
2-50
许可针对SP2创建令牌
2-52
针对SP2创建许可
针对SP2创建令牌
2-54
2-56
发送令牌（SP2）
已创建的令牌
（“机会”）
2-58
2-62
建议
2-64
建议
2-66
"Y"
2-68
2-70
OK
2-72
收费信息
2-76
确认
与步骤1-22……步
骤1-36类似

图2B

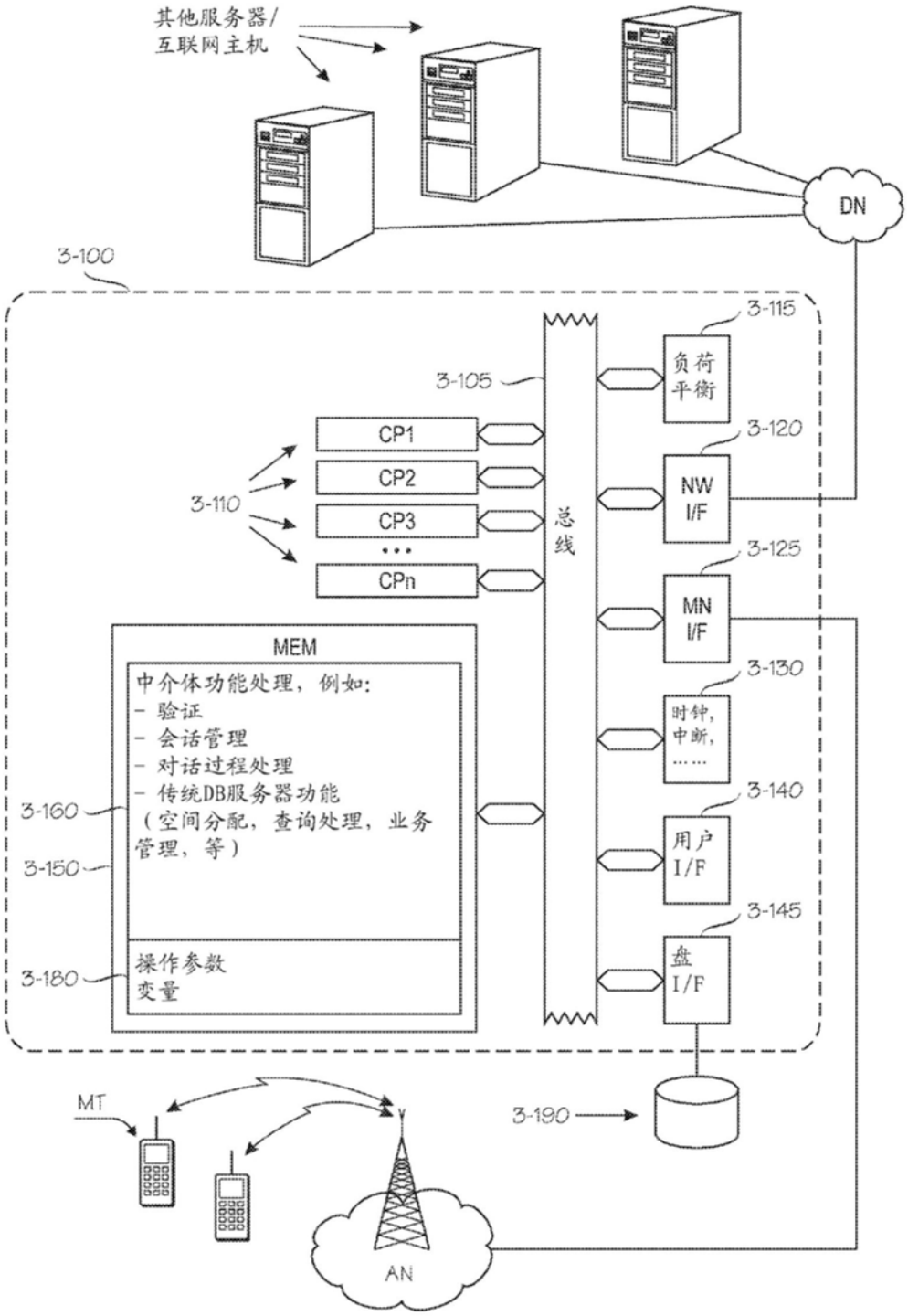

其他服务器/
互联网主机
DN
3-100
3-115
负荷
平衡
3-105
3-120
CP1
CP2
3-110
CP3
CPn
总
线
NW
I/F
3-125
MN
I/F
MEM
中介体功能处理，例如:
- 验证
- 会话管理
- 对话过程处理
- 传统DB服务器功能
（空间分配，查询处理，业务
管理，等）
3-130
时钟,
中断,
……
3-160
3-140
用户
I/F
3-150
3-145
盘
I/F
操作参数
变量
3-180
MT
3-190
AN

图3

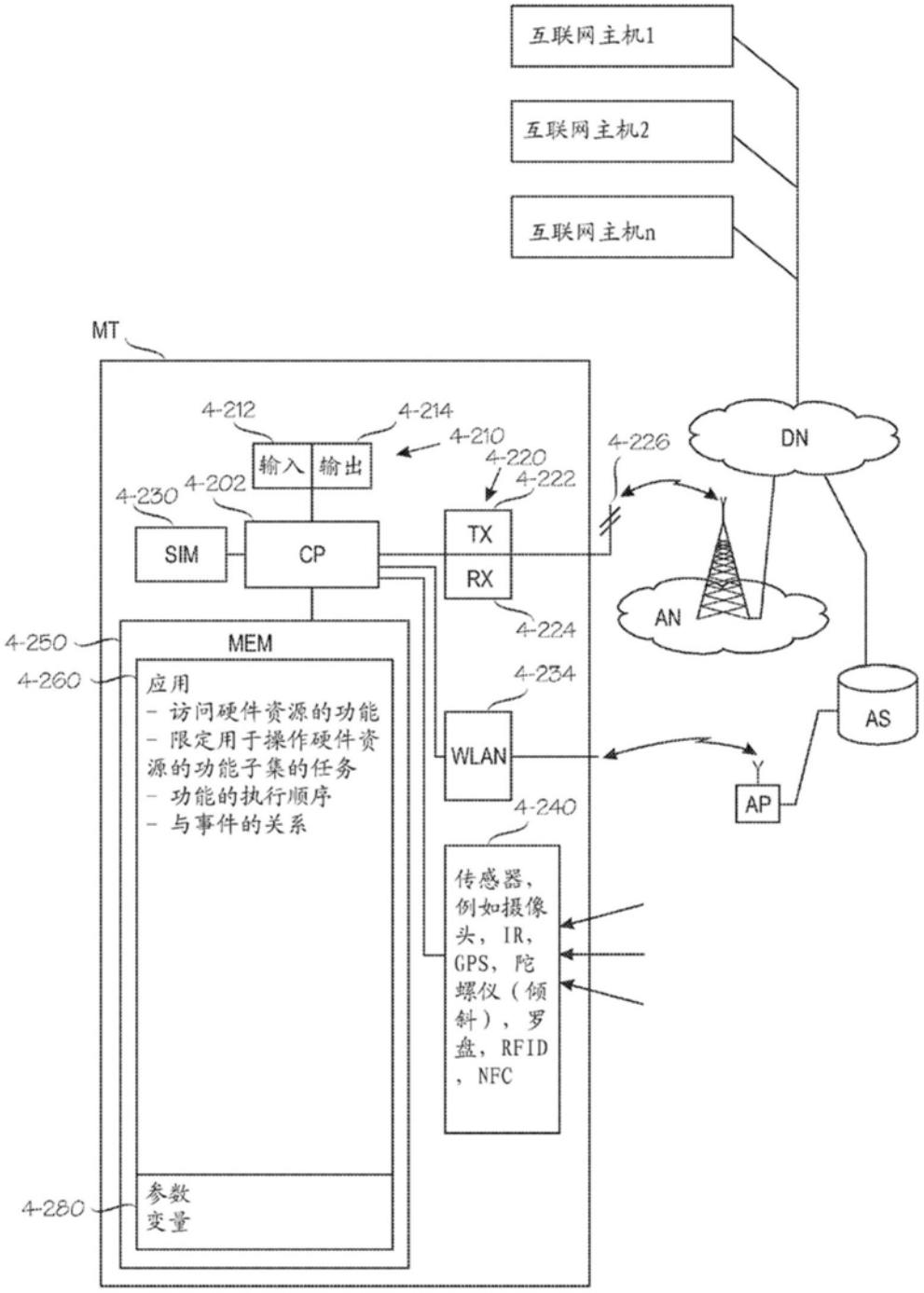

互联网主机1
互联网主机2
互联网主机n
MT
4-212
4-214
4-210
4-220
4-222
4-226
4-230
4-202
输入
输出
SIM
CP
TX
RX
DN
AN
4-224
4-250
MEM
4-260
应用
- 访问硬件资源的功能
- 限定用于操作硬件资源的功能子集的任务
- 功能的执行顺序
- 与事件的关系
4-234
WLAN
AS
AP
4-240
传感器，例如摄像头，IR，GPS，陀螺仪（倾斜），罗盘，RFID，NFC
4-280
参数
变量

图4

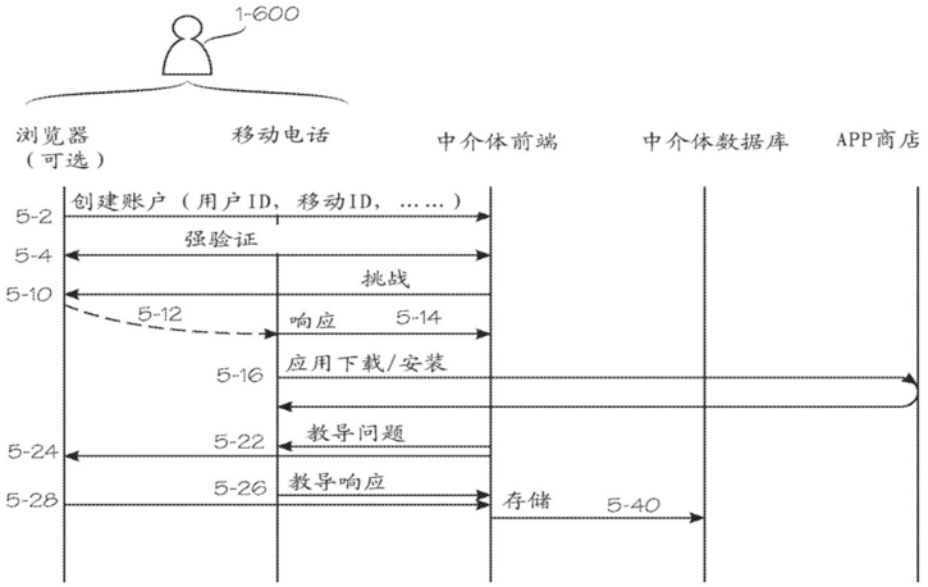

1-600
浏览器
（可选）
移动电话
中介体前端
中介体数据库
APP商店
5-2
创建账户（用户ID，移动ID，……）
5-4
强验证
5-10
挑战
5-12
响应
5-14
5-16
应用下载/安装
5-22
教导问题
5-24
5-26
教导响应
5-28
存储
5-40

图5

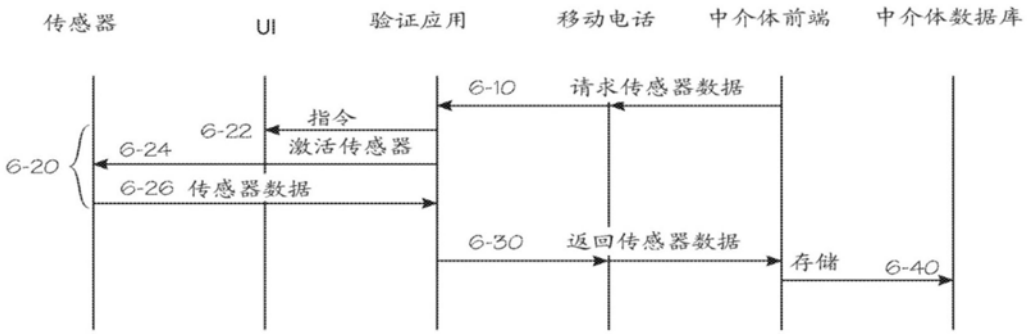

传感器
UI
验证应用
移动电话
中介体前端
中介体数据库
6-10
请求传感器数据
6-22
指令
激活传感器
6-20
6-24
6-26
传感器数据
6-30
返回传感器数据
存储
6-40

图6

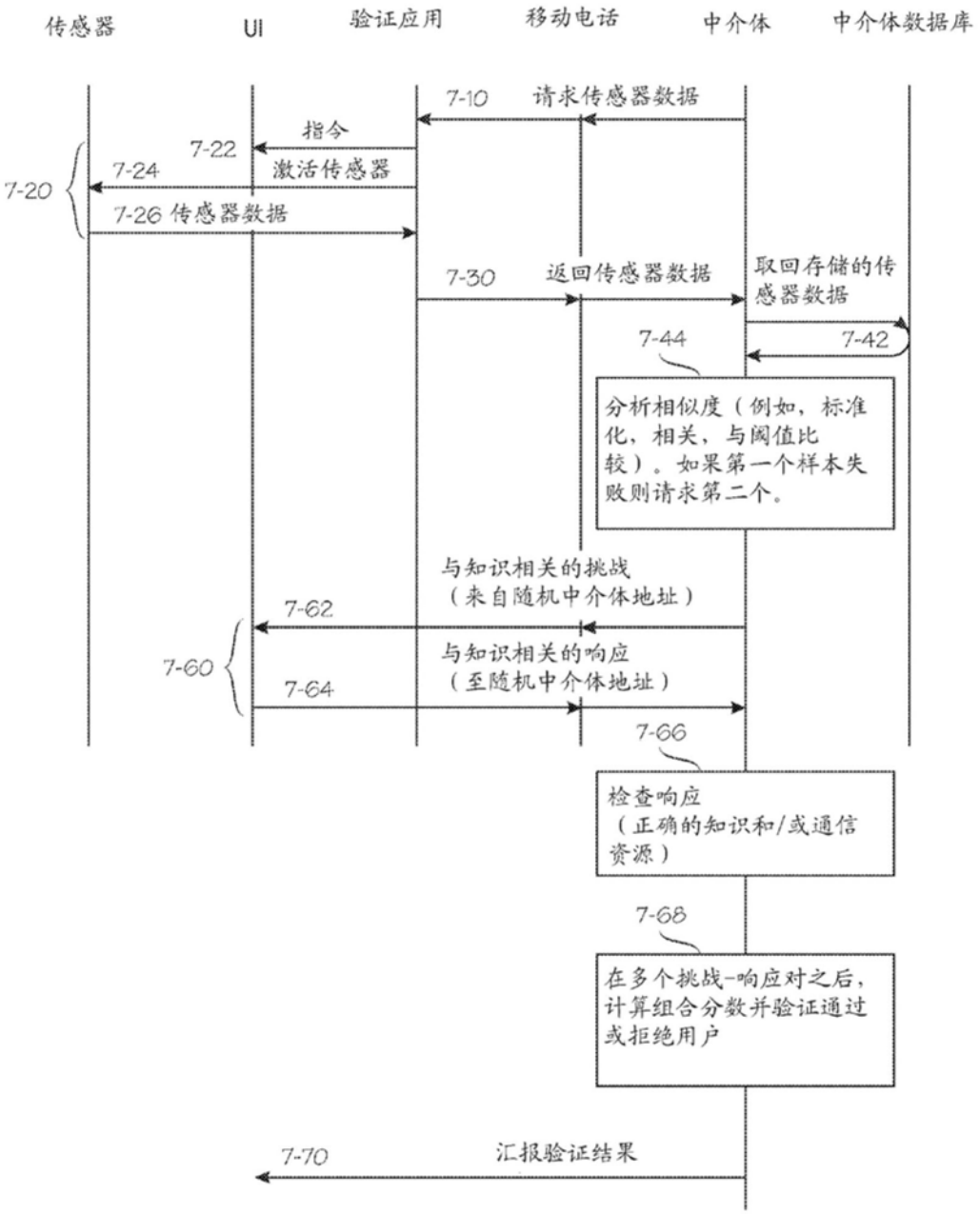

传感器
UI
验证应用
移动电话
中介体
中介体数据库
7-10
请求传感器数据
指令
7-22
激活传感器
7-24
7-20
7-26 传感器数据
7-30
返回传感器数据
取回存储的传感器数据
7-42
7-44
分析相似度（例如，标准化，相关，与阈值比较）。如果第一个样本失败则请求第二个。
与知识相关的挑战（来自随机中介体地址）
7-62
7-60
与知识相关的响应（至随机中介体地址）
7-64
7-66
检查响应（正确的知识和/或通信资源）
7-68
在多个挑战-响应对之后，计算组合分数并验证通过或拒绝用户
7-70
汇报验证结果

图7

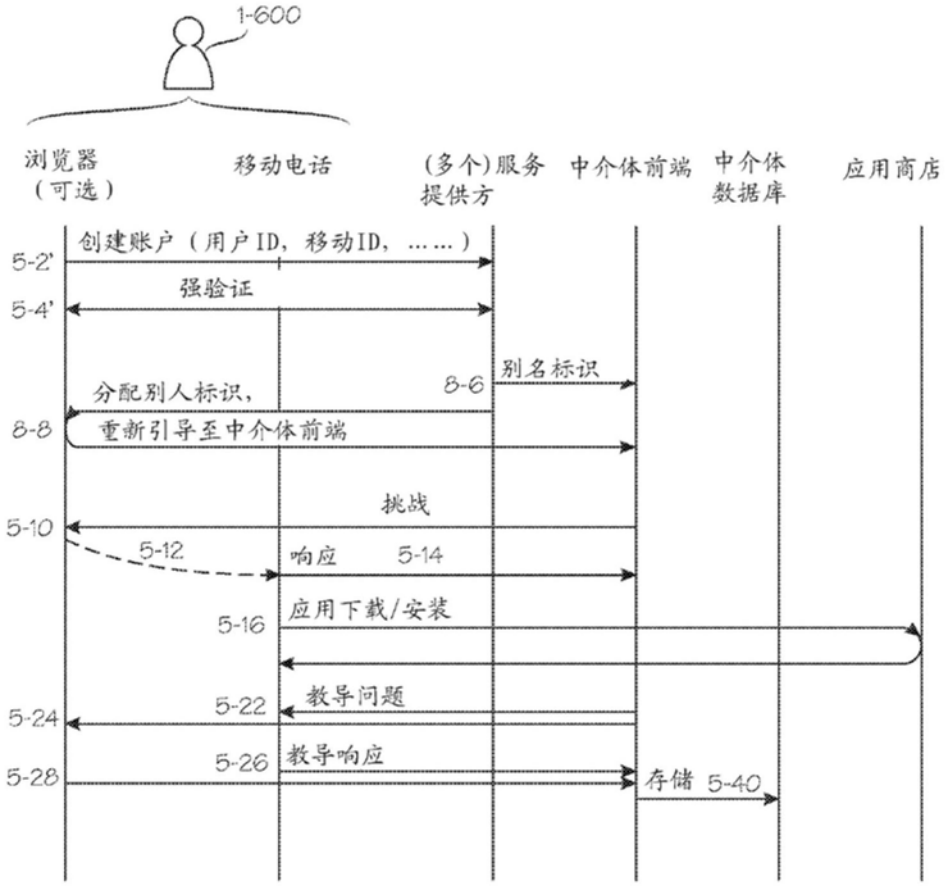

1-600
浏览器
（可选）
移动电话
(多个)服务
提供方
中介体前端
中介体
数据库
应用商店
创建账户（用户ID，移动ID，……）
5-2'
强验证
5-4'
别名标识
8-6
分配别人标识，
8-8
重新引导至中介体前端
挑战
5-10
5-12
响应
5-14
应用下载/安装
5-16
教导问题
5-22
5-24
教导响应
5-26
5-28
存储
5-40

图8