(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 102754115 B
(45)授权公告日 2018.09.18

(21)申请号 201180009132.5

(22)申请日 2011.01.19

(65)同一申请的已公布的文献号
申请公布号 CN 102754115 A

(43)申请公布日 2012.10.24

(30)优先权数据
61/296,388 2010.01.19 US

(85)PCT国际申请进入国家阶段日
2012.08.10

(86)PCT国际申请的申请数据
PCT/US2011/021734 2011.01.19

(87)PCT国际申请的公布数据
WO2011/091051 EN 2011.07.28

(73)专利权人 维萨国际服务协会
地址 美国加利福尼亚州

(72)发明人 M·林德尔西 O·布兰德 J·迪米克 B·多明格斯

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱孟清

(51)Int.Cl.
G06Q 20/40(2012.01)

(56)对比文件
WO 2009012731 A1,2009.01.29,
US 2004254894 A1,2004.12.16,
CN 101711383 A,2010.05.19,

审查员 吴文芳

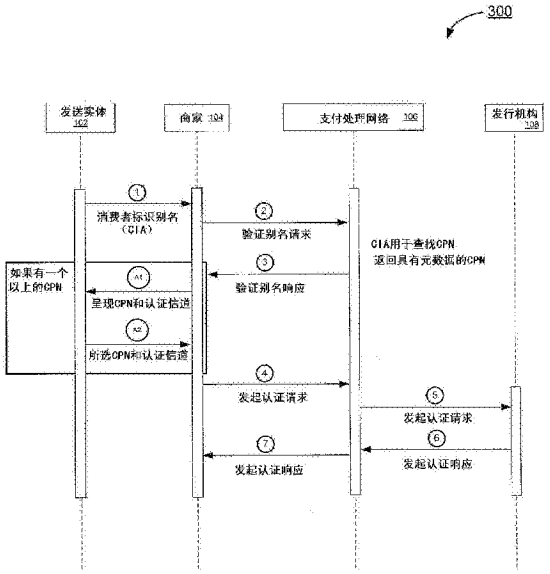
权利要求书2页 说明书15页 附图7页

(54)发明名称

远程可变认证处理

(57)摘要

公开了远程可变认证处理系统。发送实体使用别名在发起信道上发起远程支付。别名可与标识便携式消费类设备的一个或多个昵称、以及元数据相关联。元数据描述哪些信道可用于认证。发送实体选择昵称和相关联的认证信道。发送实体在所选认证信道上与发行机构进行认证。



CN 102754115 B

1.一种用于进行远程可变认证处理的方法,包括:

从参与者处接收包括别名的消息;

确定与所述别名相关联的一个或多个消费者支付昵称;

将所述一个或多个消费者支付昵称和与所述一个或多个消费者支付昵称中的每一个相关联的元数据发送给所述参与者,所述元数据描述可通过其进行对所述一个或多个消费者支付昵称的认证的认证信道,其中所述参与者将所述一个或多个消费者支付昵称和所述认证信道呈现给发送实体;以及

接收来自所述参与者的消费者支付昵称和认证信道,所述消费者支付昵称和认证信道由所述发送实体选择。

2.如权利要求1所述的方法,其特征在于,还包括:分析接收到的消费者支付昵称以确定授权实体;以及将包括认证信道标识符的认证请求消息发送给所述授权实体。

3.一种用于进行远程可变认证处理的方法,包括:

由计算机从参与者处接收包括别名的消息;

由所述计算机确定与所述别名相关联的一个或多个消费者支付昵称;

由所述计算机将所述一个或多个消费者支付昵称和与所述一个或多个消费者支付昵称中的每一个相关联的元数据发送给所述参与者,所述元数据描述可通过其进行对所述一个或多个消费者支付昵称的认证的认证信道,其中所述参与者将所述一个或多个消费者支付昵称和所述认证信道呈现给发送实体;

由所述计算机接收来自所述参与者的消费者支付昵称和认证信道,所述消费者支付昵称和认证信道由所述发送实体选择;

由所述计算机分析接收到的消费者支付昵称以确定主账号和授权实体;

由所述计算机将包括所选认证信道和所述主账号的认证请求消息发送给所述授权实体,其中所述授权实体使用所选认证信道来认证所述发送实体;

由所述计算机接收来自所述授权实体的认证响应消息;以及

由所述计算机将所述认证响应消息发送给所述参与者。

4.如权利要求1或3所述的方法,其特征在于,还包括:接收来自所述参与者的发起信道标识符;分析所述元数据以确定描述哪一个认证信道与所述发起信道标识符所描述的信道相兼容的兼容性数据;以及将所述兼容性数据发送给所述参与者。

5.如权利要求1或3所述的方法,其特征在于,所述参与者是商家。

6.如权利要求4所述的方法,其特征在于,与所述发起信道标识符所述的信道不兼容的认证信道是所述发送实体不可选择的。

7.如权利要求4所述的方法,其特征在于,与所述发起信道标识符所描述的信道不兼容的认证信道不被呈现给所述发送实体。

8.如权利要求4所述的方法,其特征在于,如果只有一个消费者支付昵称和认证信道与所述发起信道标识符相兼容,则该消费者支付昵称和认证信道用于认证所述消费者支付昵称。

9.如权利要求3所述的方法,其特征在于,所述参与者将经由发起信道向所述发送实体通知所述认证响应消息。

10.一种用于进行远程可变认证处理的系统,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括可由所述处理器执行的用于实现一种方法的代码,所述方法包括:

从参与者处接收包括别名的消息;

确定与所述别名相关联的一个或多个消费者支付昵称;

将所述一个或多个消费者支付昵称和与所述一个或多个消费者支付昵称中的每一个相关联的元数据发送给所述参与者,所述元数据描述可通过其进行对所述一个或多个消费者支付昵称的认证的认证信道,其中所述参与者将所述一个或多个消费者支付昵称和所述认证信道呈现给发送实体;以及

接收来自所述参与者的消费者支付昵称和认证信道,所述消费者支付昵称和认证信道由所述发送实体选择。

11.一种用于进行远程可变认证处理的系统,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括可由所述处理器执行的用于实现一种方法的代码,所述方法包括:

从参与者处接收包括别名的消息;

确定与所述别名相关联的一个或多个消费者支付昵称;

将所述一个或多个消费者支付昵称和与所述一个或多个消费者支付昵称中的每一个相关联的元数据发送给所述参与者,所述元数据描述可通过其进行对所述一个或多个消费者支付昵称的认证的认证信道,其中所述参与者将所述一个或多个消费者支付昵称和所述认证信道呈现给发送实体;

接收来自所述参与者的消费者支付昵称和认证信道,所述消费者支付昵称和认证信道由所述发送实体选择;

分析接收到的消费者支付昵称以确定主账号和授权实体;

将包括所选认证信道和所述主账号的认证请求消息发送给所述授权实体,其中所述授权实体使用所选认证信道来认证所述发送实体;

接收来自所述授权实体的认证响应消息;以及

将所述认证响应消息发送给所述参与者。

12.如权利要求10或11所述的系统,其特征在于,所述方法还包括:接收来自所述参与者的发起信道标识符;分析所述元数据以确定描述哪一个认证信道与所述发起信道标识符所描述的信道相兼容的兼容性数据;以及将所述兼容性数据发送给所述参与者。

远程可变认证处理

[0001] 相关申请的交叉引用

[0002] 本非临时申请根据35U.S.C.§119(e)要求2010年1月19日提交的题为“REMOTE PAYMENT INCLUDING VARIABLE AUTHENTICATIONPROCESSING(包括可变认证处理的远程支付)”的美国临时专利申请No.61/296,388的优先权,其全部内容出于所有目的通过引用整体结合于此。

[0003] 背景

[0004] 远程交易通常将更高水平的风险呈现给发送实体和商家。对于也统称为消费者的发送实体,在向发送实体无法物理地观察或访问的商家提供与支付工具相关的敏感信息时引入风险。当前,发送实体向商家提供诸如信用卡号码之类的敏感信息。发送实体处于敏感信息可被恶意用户截取和欺诈使用的风险中。对于商家,由于信用卡无法被发送实体物理地呈现给商家,因此引入风险。商家处于所提供的信用卡不被发送实体真正拥有的风险中。

[0005] 认证发送实体的系统可降低风险。然而,现有认证系统在单个认证信道上认证发送实体,并且不准许发送实体选择许多认证信道之一。现有认证系统在不公开敏感信息的情况下也不提供进行远程交易的方法。

[0006] 由此,本领域需要解决以上问题的远程可变认证过程。本发明的各个实施例单独地或共同地解决这些以及其他问题。

发明内容

[0007] 本文中所公开的本发明的各个实施例包括远程可变认证处理系统的系统、这些系统的技术架构、以及方法。远程可变认证处理系统可使用一个或多个计算机装置和数据库来实现。

[0008] 本发明的一个实施例涉及一种方法,包括:从商家接收包括别名的消息;确定与别名相关联的一个或多个消费者支付昵称;以及将一个或多个消费者支付昵称和与一个或多个消费者支付昵称中的每一个相关联的元数据发送给所述商家,元数据描述通过其可进行对一个或多个消费者支付昵称的认证的认证信道,其中商家将一个或多个消费者支付昵称和认证信道呈现给发送实体。

[0009] 本发明的另一实施例涉及一种方法,用于:从商家处接收发起信道标识符;分析元数据以确定描述哪一个认证信道与发起信道标识符所描述的信道相兼容的兼容性数据;以及将兼容性数据发送给商家。

[0010] 本发明的另一实施例涉及一种方法,其中如果只有一个消费者支付昵称和认证信道与发起信道标识符相兼容,则该消费者支付昵称和认证信道用于认证消费者支付昵称。

[0011] 本发明的这些以及其他实施例将在下文中更详细地描述。

附图说明

[0012] 图1是根据示例实施例的远程可变认证处理系统。

[0013] 图2是根据示例实施例的远程可变认证处理系统的更详细框图。

[0014] 图3是根据示例实施例的远程可变认证发起过程的过程流。

[0015] 图4是根据示例实施例的基于web的远程可变认证过程的过程流。

[0016] 图5是根据示例实施例的其中发起信道与认证信道不同的远程可变认证过程的过程流。

[0017] 图6是根据示例实施例的其中发起信道与认证信道相同的远程可变认证过程的过程流。

[0018] 图7是根据示例实施例的计算机装置的示图。

[0019] 详细描述

[0020] 本发明的各个实施例涉及进行远程可变认证过程的系统、这些系统的架构、以及方法。

[0021] 在特定实施例中，远程可变认证过程标识发送实体，确定发送实体从可能的多个便携式消费类设备和认证信道中选出的便携式消费类设备和认证信道，并且经由所选的认证信道进行认证，而不将敏感信息暴露给商家。

[0022] 在以下的描述中，对“商家”进行引用。商家可以是“参与者”的一个示例。参与者的其他示例可包括接收来自发送实体的信息(诸如别名或其他标识信息)的实体。这些实体可返回本地存储或通过查询支付处理网络获取的支付工具信息。参与者可发送和接收发送实体便携式消费类设备信息，并且可操作地与商家通信。

[0023] 在以下的描述中，对“发行机构”进行引用。发行机构可以是“授权实体”的一个示例。授权实体可以是可授权转账交易的实体。授权实体的其他示例可包括管理或主存发送实体账户的实体，诸如在线额度存储账户供应商、银行、或转账服务。

[0024] 发送实体可通过向商家提供“消费者身份别名”(“CIA”)(也称为别名)来发起认证以标识他自己或她自己。然后，商家可向支付处理网络提供CIA。支付处理网络可查找CIA以确定与该CIA相关联的消费者支付昵称(“CPN”)，其中消费者支付昵称标识诸如信用卡之类的便携式消费类设备。CPN可用元数据来标记，元数据描述CPN标识的便携式消费类设备可通过其认证的认证信道和可通过其发起认证的发起信道等参数。支付处理网络可将消费者支付昵称和元数据发送给商家，该商家随后将该数据显示给发送实体。然后，发送实体可选择消费者支付昵称和认证信道。然后，所选消费者支付昵称和认证信道被传达给商家、支付处理网络、以及发行机构。然后，发送实体可经由所选认证信道与发行机构进行认证。然后，商家可通过查询支付处理网络和发行机构来验证发送实体成功地与发行机构进行了认证。在成功验证之后可以是支付交易或转账。

[0025] 例如，为了降低发送实体和商家两者的风险，发送实体可在优选认证信道上认证，而不暴露诸如信用卡号码之类的敏感信息。作为示例，发送实体可经由商家网站向商家提供诸如“ted@ted.com”之类的CIA以支付商家的商品。然后，商家可用“ted@ted.com”查询支付处理网络，该支付处理网络返回与CIA“ted@ted.com”相关联的发送实体的实际信用卡(诸如“我的蓝卡”和“我的红卡”)的昵称和元数据。元数据可指示“我的蓝卡”可在SMS上认证而“我的红卡”可通过web认证。发送实体可选择“我的蓝卡”和SMS认证，因为他或她无法在此刻访问计算机终端。该选择最终传达给发行机构，该发行机构要求发送实体使用口令在SMS上认证“我的蓝卡”。发送实体可将SMS消息与口令一起发送给发行机构来进行认证。商家可验证发送实体与发行机构进行认证，并且随后更有信心地继续支付交易。

[0026] 如本文中所使用的，“便携式消费类设备”可以是信用卡、借记卡、移动电话、预付卡、移动应用、支付工具、专属应用、或者能够转移资金的任何便携式设备或软件应用。这些设备可包括接触式或非接触式智能卡、普通信用卡或借记卡(有磁条但没有嵌入式微处理器)、钥匙链设备(诸如可从Exxon-Mobil公司购得的Speedpass™)等。便携式消费类设备的其他示例包括蜂窝电话、个人数字助理(PDA)、寻呼机、支付卡、安全卡、门禁卡、智能介质、应答器等，其中这些设备可包括嵌入或集成的非接触式芯片或类似元件。

[0027] 远程可变认证过程可支持在发送实体和商家之间进行的支付交易，并且可在这些支付交易之前进行，其中发送实体使用便携式消费类设备向商家进行支付。例如，支付交易可将来自与发送实体信用卡相关联的账户的资金转移到商家的商家银行账户，并且可能需要对该支付交易的发行机构授权。这些支付交易的示例可包括使用信用卡向在线商家购物。

[0028] 远程可变认证过程还可支持便携式消费类设备之间的转账，并且可在这些转账之前进行。在示例实施例中，转账将来自与便携式消费类设备相关联的一个账户的资金转移到与另一便携式消费类设备相关联的另一账户。在示例实施例中，转账可将来自一个信用卡账户的资金转移到另一信用卡账户。在另一实施例中，账户可与诸如移动电话或智能卡之类的移动设备相关联。在示例实施例中，账户可与支付处理网络相关联、和/或可由发行实体或银行保持。

[0029] 远程可变认证过程可诸如通过使用CIA来方便对支付交易和转账中所涉及的发送实体的认证，而不暴露敏感信息。如本文中所使用的，CIA可以是诸如用户名之类的字母数字值，并且可以是静态或动态的。CIA可用于标识发送实体而不是共享敏感信息，从而保护隐私并减少欺诈的可能性。CIA可与一个或多个便携式消费类设备相关联。在又一实施例中，CIA可以是诸如电话号码或电子邮件地址之类的可验证值。例如，在转账交易中，发送实体可从CIA“ted@ted.com”发送金钱，而不提供信用卡号码。

[0030] CIA可与一个或多个便携式支付昵称相关联。如本文中所使用的，“消费者支付昵称”(“CPN”)可以是字母、数字和字符的任何组合，可以是字母数字串、令牌，或者可以是静态或动态的，并且可标识便携式消费类设备。CPN可以是发送实体定义的昵称，诸如“我的红卡”、“我的黄点卡”等。发送实体可向支付处理网络登记以使CIA与一个或多个CPN相关联。CPN可用于标识便携式消费类设备，而不泄漏诸如信用卡截止日期、CVV2、或者也称为永久账号或个人账号的主账号(“PAN”)之类的敏感信息。例如，发送实体可与商家共享诸如“第一张信用卡”之类的CPN以标识和使用便携式消费类设备，而不暴露该便携式消费类设备的PAN、信用卡截止日期、或者其他敏感信息。

[0031] CPN可用元数据来标记，或者可与元数据相关联。CPN的元数据可描述一个或多个认证信道等参数。元数据还可描述发起信道、以及发起信道和认证信道对。发起信道是发送实体可通过其请求发起对便携式消费类设备的认证的信道。在示例实施例中，发起信道是发送实体经由其与商家通信以发送CIA并且发送和接收关于CPN和元数据的信道。认证信道可以是实际上通过其对便携式消费类设备进行认证的信道。在示例实施例中，认证信道是发送实体和发行机构经由其通信以共享口令以及其他认证数据的信道。

[0032] 发起信道和认证信道对可描述通过其发送实体可分别发起和进行对特定便携式消费类设备的认证的发起信道和认证信道的有效组合。例如，发送实体可经由SMS发起认

证，并且可使用CSR来进行认证。在此情况下，SMS/CSR是指示对于特定便携式消费类设备，认证发起可经由SMS传达而认证可使用IVR过程进行的发起信道和认证信道对。在示例实施例中，如果认证信道未在具有特定发起信道的发起信道和认证信道对中列出，则在该特定发起信道用于发起认证时该认证信道不可用于认证便携式消费类设备。在此情况下，认证信道与发起信道不兼容。元数据可包括描述认证信道是否与发起信道相兼容的指示符。在又一实施例中，元数据可只描述认证信道。元数据还可指示对于特定便携式消费类设备哪一个认证信道是优选认证信道。元数据还可指示CPN中的每一个对于经由“一次性口令”的认证是否合格。一次性口令可以是对单次交易或认证对话有效的口令。

[0033] 如本文中所使用的，“发起信道”可指用于开始认证过程的通信路径。“认证信道”可指用于认证实体的通信路径。发起和认证信道可使用任何合适的过程或设备。例如，发起信道和认证信道可使用以下的任一个：web、移动web、移动应用、短消息收发服务（“SMS”）、交互式语音响应（“IVR”）过程、非结构化辅助服务数据（“USSD2”）、和/或客户服务代表（“CSR”）。例如，如果发起信道使用SMS而认证信道使用CSR，则发送实体可经由SMS发起认证并且使用CSR发起认证。在示例实施例中，发起信道可与认证信道相同。在另一实施例中，发起信道与认证信道不同。在又一实施例中，有效信道的任何组合可用作发起和认证信道。在示例实施例中，认证信道还可标识发送实体根据其可进行联系的地址、位置、或者数量。例如，认证信道还可指示发送实体电话号码、IP地址、应用序列号等。

[0034] CPN可与PAN、或者其他便携式消费类设备标识信息相关联。可分析PAN或者其他便携式消费类设备标识信息以解析发行机构。例如，可分析PAN以导出发行机构标识号。发行机构可以是将便携式消费类设备发行给发送实体的发行银行。在示例实施例中，发行机构还提供认证服务。发送实体可在发送实体所选的认证信道上发起与发行机构的认证。在又一实施例中，发送实体向发行机构登记。

[0035] 远程可变认证处理系统可包括发送实体、商家、支付处理网络和发行机构（以及与以上实体相关联的计算机装置）。发送实体可经由发起和认证信道与商家、支付处理网络、以及发行机构通信。例如，发送实体可经由商家网站发送消息。发送实体可通过向商家提供CIA来标识他自己或她自己。然后，商家可查询支付处理网络以验证该CIA已向支付处理网络注册并且该CIA与一个或多个CPN相关联。

[0036] 支付处理网络可通过查找CIA并返回与该CIA相关联的CPN列表及其相关联的元数据来对商家作出响应。在示例实施例中，将所有相关联的CPN发送给商家。在又一实施例中，将所有相关联的CPN发送给商家，但是其元数据指示与发送实体用来发起认证的发起信道不兼容的认证信道的那些CPN被标记为不兼容。在另一实施例中，支付处理网络可分析该CPN列表并且只返回其元数据指示与发送实体用来发起认证的发起信道兼容的认证信道的那些CPN。

[0037] 如果一个以上的CPN与所提供的CIA相关联，则商家可将一个或多个CPN及其认证信道一起呈现给发送实体。有可能多次地示出相同的CPN，每一认证信道一次。一个或多个CPN可经由发起信道发送给发送实体。在示例实施例中，商家只显示CPN、以及与商家和发送实体所使用的发起信道兼容的认证信道。在又一实施例中，只有兼容的认证信道才可由发送实体选择。然后，发送实体可选择要在认证过程中使用的一个CPN和认证信道，并将该选择经由认证信道发送给商家。如果没有CPN与所提供的CIA相关联，则可终止交易。如果只有

一个CPN和认证信道与所提供的CIA相关联，则使用该CPN和认证信道、且可能是没有CPN列表被呈现给发送实体。在该实例中，可将CPN和认证信道呈现给发送实体以供批准。有可能没有CPN或认证信道兼容且被呈现给发送实体。

[0038] 在商家确定要在认证过程中使用的一个CPN和认证信道之后，商家就将消息发送给支付处理网络以发起认证请求。在示例实施例中，商家可向支付处理网络请求发送实体可重定向来进行认证的地址。在又一实施例中，商家可向支付处理网络通知发送实体所选的认证信道，该认证信道随后可通过支付处理网络进一步传达给发行机构。

[0039] 在支付处理网络接收到来自商家的消息之后，支付处理网络分析该一个CPN并导出发行机构。支付处理网络可分析CPN，并且确定相关联的PAN或便携式消费类设备且随后确定发行机构。在确定发行机构之后，支付处理网络可向发行机构发送标识发送实体、便携式消费类设备、以及认证信道的消息。在示例实施例中，支付处理网络可将CIA和CPN发送给发行机构以保护敏感信息。

[0040] 在接收到来自支付处理网络的消息之后，发行机构可分析这些内容并确定相关联的便携式消费类设备、发送实体、以及认证信道。然后，发行机构可准备响应消息以返回至支付处理网络。响应消息可指示与发行机构的认证将开始，或者其可指示商家应当重定向发送实体以便于发送实体认证的认证地址。支付处理网络可接收来自发行机构的消息，并将具有类似内容的另一消息发送给商家。

[0041] 在商家接收来自支付处理网络的消息之后，过程流根据发送实体所选的发起信道和认证信道而变化。发送实体可能已选择了基于web的认证信道和基于web的发起信道、与该发起信道不同的认证信道、或者与该发起信道相同的认证信道。

[0042] 在基于web的认证情形中，商家将认证地址传达给发送实体，并将发送实体重定向到认证地址。这可将发送实体定向到由发行机构操作的认证系统。在此，发送实体可通过提供诸如口令之类的信息与发行机构进行认证。在认证之后，发行机构随后可将发送实体重定向回商家。然后，商家可查询支付处理网络来查询发行机构，以验证发送实体成功地与发行机构进行了认证。如果发送实体成功认证并且描述成功认证的消息被中继给商家，则商家将认证的确认发送给发送实体，并且可继续授权支付交易或转账。

[0043] 在发起信道和认证信道不同的情形中，发行机构随后将通过发送实体所选的认证信道联系发送实体。然后，发行机构和发送实体将通信以诸如通过提供口令来认证发送实体。发行机构可将指示认证结果的认证响应发送给发送实体。同时，商家可继续查询支付处理网络来查询发行机构，以确定发送实体是否已成功地认证。商家可查询支付处理网络达设定时间段，同时等待发送实体在认证信道上认证。在商家从发行机构和支付处理网络处接收到发送实体已成功认证的通知之后，商家随后将认证的确认发送给发送实体，并且可继续授权支付交易或转账。

[0044] 发起信道和认证信道相同的情形可与发起信道和认证信道不同的情形类似地操作，不同之处在于，发行机构联系发送实体在与发起信道相同的信道上发起认证。

[0045] 本发明的各个实施例的其他具体示例在下文中更详细地描述。

[0046] I.系统

[0047] 图1是根据示例实施例的远程可变认证处理系统100。远程可变认证处理系统100包括发送实体102、商家104、支付处理网络106、以及发行机构108。虽然只示出一个发送实

体102、一个商家104、一个支付处理网络106、以及一个发行机构108，但是在基于令牌的交易认证系统100中可存在任何合适数量的这些实体中的任一个。

[0048] 发送实体102可以是使用便携式消费类设备来进行支付交易或转账的消费者，并且还可操作包括移动设备的一个或多个用户设备，该移动设备可包括移动电话。发送实体102可以是个人、或者诸如能够购买商品或服务的公司之类的机构。

[0049] 如本文中所使用的，商家104可指能与发送实体102进行交易的任何合适的一个或多个实体。将商品和服务出售给发送实体102的商家104可具有物理位置。商家104可使用电子商务来允许商家通过因特网进行交易。商家104的其他示例包括百货商店、加油站、药店、杂货店、或者其他合适的商店。

[0050] 支付处理网络106是指具有与关联于便携式消费类设备的账户相关的信息的合适实体的网络。该信息包括与便携式消费类设备上的账户相关联的数据，诸如简档信息、数据、CIA、CPN、元数据、以及其他合适的信息。

[0051] 支付处理网络106可具有或操作服务器计算机，并且可包括数据库。数据库可包括用于存储信息和便于信息检索的任何硬件、软件、固件、或者前三者的组合。同样，数据库可使用各种数据结构、排列和编译中的任一个来存储信息和便于信息检索。服务器计算机可耦合到数据库，并且可包括用于对来自一个或多个客户机计算机的请求提供服务的任何硬件、软件、其他逻辑、或者前三者的组合。服务器计算机可使用各种计算结构、排列和编译中的任一个来对来自一个或多个客户机计算机的请求提供服务。

[0052] 支付处理网络106可包括用于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、以及操作。示例性支付处理网络106可包括VisaNet™。包括VisaNet™的网络能够处理信用卡交易、借记卡交易、以及其他类型的商业交易。具体而言，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106可使用包括因特网在内的任何合适的有线或无线网络。

[0053] 发行机构108是指可打开并维护与发送实体102所使用的便携式消费类设备相关联的账户的任何合适的实体。发行机构108的一些示例可以是银行、诸如零售店之类的商业实体、或者政府实体。发行机构108可提供认证服务，诸如允许发送实体102提供口令来进行认证。

[0054] 发送实体102可与商家104通信。在示例实施例中，商家104可以是发送实体102经由因特网或移动网络与其通信的在线商家。发送实体102可经由发起信道或通信网络与商家104通信。发送实体102可与商家104通信以提供和/或接收CIA、CPN、发起信道标识符、要重定向到的认证地址、以及成功认证的确认或者所选CPN和认证信道。

[0055] 发送实体102还可与发行机构108通信。发送实体102在认证信道上与发行机构108通信。在示例实施例中，发送实体102可通过提供口令与发行机构108进行认证。在示例实施例中，发送实体102的便携式消费类设备可已由发行机构108发行。

[0056] 商家104和发行机构108可与支付处理网络106通信。商家104可与支付处理网络106通信，以确定与CIA相关联的CPN、确定与CPN相关联的发行机构、接收认证发送实体所需的各种密钥和令牌、以及接收CPN元数据。商家104可在通信网络(诸如因特网、或者认证/发起信道中的任一个)上与支付处理网络106通信。

[0057] 支付处理网络106可与发行机构108通信，以确定重定向发送实体102的认证地址

并验证发送实体102成功地与发行机构108进行了认证。支付处理网络106还可与发行机构108通信，以传达发送实体102想要在其上进行认证的认证信道以及想要认证的CPN/便携式消费类设备。支付处理网络106可将账户资助交易消息和原始信用交易消息发送给发行机构108和商家的银行以完成转账。支付处理网络106还可将取款和存款消息发送给发行机构108/商家银行以完成支付交易。发行机构108可在通信网络(诸如因特网、或者认证/发起信道中的任一个)上与支付处理网络106通信。

[0058] 发送实体102还可与支付处理网络106通信。发送实体102可在认证过程之后与支付处理网络106通信以进行支付交易或转账，并且还可在认证之前与支付处理网络106通信以诸如通过提供CIA和CPN数据注册认证服务。在示例实施例中，发送实体102可在认证过程期间与支付处理网络106通信以提供和接收认证数据。发送实体102可在通信网络(诸如因特网、或者认证/发起信道中的任一个)上与支付处理网络106通信。

[0059] 商家104还可与发行机构108通信。在示例实施例中，商家104可从发行机构108接收认证请求状态。商家104可在通信网络(诸如因特网、或者认证/发起信道中的任一个)上与发行机构108通信。

[0060] 远程可变认证处理系统100中的实体之间的通信也可经由web、移动网络、内联网、SMS/IVR、普通老式电话系统、电子邮件、USSD-2、API、定制消息、专属应用、通信网络、或者所列出的发起或认证信道中的任一个来进行。

[0061] 图2是根据示例实施例的远程可变认证处理系统200的更详细框图。远程可变认证处理系统200可包括发送实体102、商家104、发行机构108、接入控制服务器210、第三方认证器212、支付处理网络106、以及数据库224。

[0062] 商家104可包括商家插件204和购物车202。商家104可经由商家插件204与支付处理网络106通信。商家插件204可以是实现支持认证协议(诸如图3-6中所述的协议)的逻辑的模块。商家插件204可包括验证别名模块208和发起认证模块206。这些模块可接收来自支付处理网络106的消息，并将消息发送给支付处理网络106。验证别名模块208可将请求CPN和提供CIA的消息发送给支付处理网络106。验证别名模块208还可处理响应，并管理CPN和认证信道向发送实体102的呈现。发起认证模块206可将请求认证地址、或描述发送实体102所选的认证模块的消息发送给支付处理网络，并且可诸如通过将发送实体102重定向到认证地址来分析任何响应。购物车202可以是呈现或存储发送实体102希望从商家104购买的物品或商品列表的模块。验证别名模块218和发起认证模块206可经由商家插件204通信。商家插件204可经由因特网、或者发起信道/认证信道中的任一个、并且通过支付处理网络的接口214与支付处理网络106通信。

[0063] 发行机构108可经由接入控制服务器210或第三方认证器212与支付处理网络接口214通信。接入控制服务器210是由发行机构108操作或推动的可认证便携式消费类设备的持有者的服务器。如果发行机构108不拥有接入控制服务器210或不直接支持认证，则第三方认证器212可被发行机构108用来执行认证操作。第三方认证器212可以是可针对发行机构108执行认证步骤的服务器或服务供应商。接入控制服务器210和第三方认证器212可通过支付处理网络接口214、并且经由因特网、或者发起或认证信道中的任一个与支付处理网络106和发行机构108通信。

[0064] 支付处理网络可包括接口214、认证模块216、以及数据库224。支付处理网络接口

214可拥有支持各种通信协议的模块。支付处理网络接口214可拥有接收、解析和分析经由XML、HTTP、SOAP、以及其他协议发送的消息的XML/HTTP和SOAP(简单对象接入协议)模块。XML/HTTP和SOAP模块还可以各种格式且根据诸如XML、HTTP和SOAP之类的各种协议封装和创建发出消息。

[0065] 认证模块216可包括验证别名模块220、发起认证模块222、以及认证状态模块223。发起认证模块222可接收和发送与验证CIA和发起认证相关的消息。验证别名模块220可从商家104接收请求CIA的消息,诸如从商家验证别名模块208发送的请求CPN和元数据的消息。在示例实施例中,验证别名模块220可从商家104接收包括CIA的验证别名请求消息。验证别名模块220可通过发送包括CPN以及相关联的元数据的消息来对商家104作出响应。CPN和CIA数据可通过验证别名模块220存储、以及从数据库224中检索。验证别名模块220可基于发起信道标识符和元数据确定认证信道的兼容性。

[0066] 支付处理网络106还可以是提供远程服务的远程目录。

[0067] II.方法

[0068] A.认证发起

[0069] 图3是根据示例实施例的远程可变认证过程的过程流。在操作1,发送实体102通过将包括CIA的消息发送给商家104来发起认证。该消息经由发起信道发送。出于安全或方便的因素,发送实体102可能偏好提供CIA而非PAN。发送实体102还可向商家104提供附加信息,诸如标识该信息经由其发送的发起信道的发起信道标识符。该消息可经由购物车202发送。例如,该消息可包含CIA“ted@ted.com”,并且可包含描述web信道的发起信道标识符。发起信道标识符还可描述用于联系发送实体102的具体方法,诸如电话号码、IP地址等。

[0070] 在接收到在操作1从发送实体102发送的消息之后,商家104可分析接收到的消息的内容。发送实体102发送的消息可由商家插件204和验证别名模块208接收。在操作2,商家随后可将该消息中接收到的CIA发送给支付处理网络106以请求与CIA相关联的CPN。该消息还可包括发起信道标识符。该消息可由验证别名模块208发送。在示例实施例中,该消息是验证别名请求消息。例如,商家104可将具有CIA“ted@ted.com”的消息发送给支付处理网络106,并且发起信道标识符会描述web信道。

[0071] 支付处理网络106接收在操作2从商家104发送的消息,并分析接收到的消息的内容。该消息可由支付处理网络接口214接收,并且由交易模块216和验证别名模块220分析。验证别名模块220可查找CIA,并且通过用CIA在数据库224中查询相关联的CPN来检索相关联的CPN。在示例实施例中,在通过支付处理网络106的发送实体登记过程期间CPN与CIA相关联,其中发送实体102可创建CIA,并且通过创建每一便携式消费类设备的CPN使一个或多个便携式消费类设备与CIA相关联。例如,支付处理网络106可在数据库224中查找CIA“ted@ted.com”,并且确定CPN“我的红卡”、“我的蓝卡”和“我的绿色借记卡”相关联。

[0072] 另外,支付处理网络106可从数据库224中检索指示CPN所表示的便携式消费类设备可通过哪些认证信道认证的CPN元数据。在示例实施例中,在给定通过其发起认证的发起信道时确定哪些认证信道可用的发起信道和认证信道对中描述认证信道。例如,在SMS或web信道上而不是经由CSR信道发起认证时,经由SMS信道的认证可用。在又一实施例中,在没有伴随的发起信道的情况下描述认证信道。作为示例,元数据可描述在认证经由web发起时,CPN“我的蓝卡”可由SMS信道认证。

[0073] 在操作3，支付处理网络106可将消息发送给商家，该消息包括与在操作2发送给商家104的CIA相关联的CPN和元数据。该消息可由验证别名模块220发送、由商家插件204接收、并且由商家验证别名模块208分析。在示例实施例中，支付处理网络106可只发送在基于web的认证信道下兼容的CPN和认证信道。在另一实施例中，支付处理网络106和验证别名模块220分析发起信道标识符，并且只将兼容的CPN和认证信道发送给商家104。在又一实施例中，支付处理网络106和验证别名模块220可分析发起信道标识符，并且在将CPN元数据发送给商家104之前将不兼容的信道标记为不兼容。在示例实施例中，该消息是验证别名响应消息。该消息还可包括发起信道标识符。例如，支付处理网络106可发送具有CPN“我的蓝卡”以及认证信道“SMS”和“web”的消息。

[0074] 商家104可从支付处理网络106接收在操作3发送的包含CPN和元数据的消息，并且可分析该消息。该消息可由商家插件204和验证别名模块208接收。商家104可将CPN和认证信道呈现给发送实体102。如果接收到一个以上的兼容的CPN和认证信道，则在操作A1，可将兼容的CPN和认证信道呈现给发送实体102。在操作A2，发送实体102可选择一个CPN和认证信道，并将该选择发送回商家104。发送实体102还可在选择认证信道时提供可描述在认证方法期间如何联系发送实体102的信息，诸如电话号码或IP地址。在示例实施例中，在给定发送实体发起信道的情况下，可只将兼容的CPN和认证信道呈现给发送实体102。如果CPN都不合格，则可取消认证过程。如果只有一个CPN和认证信道兼容，则使用该CPN，并且该CPN可请求发送实体102在继续认证之前授权。可向发送实体102呈现针对CPN的偏好认证信道(如果存在这种偏好)。商家104可经由发起信道与发送实体102通信。该消息可经由验证别名模块208发送。例如，可向发送实体102呈现CPN“我的蓝卡”可使用“SMS”或“web”来认证。然后，发送实体102可选择“我的蓝卡”和“SMS”。发送实体102还可选择发送SMS的电话号码。

[0075] 在操作4，商家104可将标识发送实体102所选的CPN和认证信道的消息发送给支付处理网络106。该消息可经由商家插件204的验证别名模块208发送。该消息还可包括标识发送实体102的信息和发起信道标识符。在示例实施例中，该消息可以是发起认证请求消息。例如，该信息可包括CPN“我的蓝卡”和认证信道“SMS”、以及发送实体电话号码。

[0076] 支付处理网络106可接收在操作4从商家104发送的消息，并分析消息内容。支付处理网络接口214可接收该消息，并且发起认证模块222可分析该消息。可分析CPN以确定发行机构108。CPN可用于查询数据库224以确定相关联的PAN，并且可从PAN导出发行机构标识号。

[0077] 在操作5，支付处理网络106可将消息发送给发行机构108。该消息可由发起认证模块222发送。该消息可包括用户所选的CPN和认证信道。该消息还可包括与CPN相关联的PAN、以及发起信道标识符。该消息还可包括CIA。发送给发行机构108的消息可请求定向发送实体102的认证地址以便于发送实体102与发行机构108进行认证、或者请求在所选的认证信道上认证。例如，针对CPN“我的蓝卡”，支付处理网络106可发送指示发送实体102希望经由SMS认证的消息。在示例实施例中，该消息是由发起认证模块222发送的发起认证请求消息。

[0078] 发行机构108接收在操作5从支付处理网络106发送的消息，并分析该内容。发行机构108可使用CPN来确定认证地址。认证地址可定向到发行机构108、发行机构接入控制服务器210、或者第三方认证器212。发行机构108还可准备在所选认证信道上认证发送实体102。然后，发行机构108可将消息发送给支付处理网络106。在示例实施例中，该消息可包括认证

地址。在又一实施例中，该消息可确认在所选认证信道上的认证将开始。在示例实施例中，该消息是发起认证响应消息。例如，该消息可包括认证地址“authenticate.ted.com.””。

[0079] 支付处理网络106接收在操作6从发行机构108发送的消息，并且可分析该内容。该消息可由支付处理网络接口214接收，并由发起认证模块222分析。在操作7，支付处理网络106将消息发送给商家104。该消息可由发起认证模块222发送。在示例实施例中，该消息可包括认证地址。在又一实施例中，该消息可确认在所选认证信道上的认证将开始。该消息可经由接入控制服务器210或第三方认证器212发送。在示例实施例中，该消息是发起认证响应消息。

[0080] 支付处理网络104接收在操作7从支付处理网络106发送的消息，并且可分析其内容。该消息可由商家插件204接收，并由发起认证模块206分析。在该点之后，操作根据发起信道和认证信道而变化。当发起信道和认证信道相同且都不基于web时、以及当发起信道和认证信道不同时，分开的操作过程流可适用于基于web的发起和认证。基于web的发起和认证在图4中进一步描述。发起信道和认证信道不同时的认证在图5中进一步描述。发起信道和认证信道相同时的认证在图6中进一步描述。

[0081] B基于web的认证

[0082] 图4是根据示例实施例的基于web的远程可变认证过程的过程流。该过程流可描述发起和认证信道是基于web(诸如基于因特网或移动web通信)的情形。

[0083] 从图3结束的地方开始，在操作8a，商家104向发送实体102发送将发送实体102重定向到认证地址的消息。该消息可由商家插件204和发起认证模块206发送。商家104可发送服务器侧HTTP重定向(30X代码)。认证地址可将发送实体102从商家网页(未示出)重定向到发行机构108、接入控制服务器210、或第三方认证器212。该消息可包括标识发送实体102、CPN、发起信道标识符、以及认证信道的信息。在操作9a，发送实体102将请求认证的消息发送给发行机构108。该消息可经由发送实体102所选的认证信道发送。

[0084] 发行机构108接收在操作9a由发送实体102发送的消息，并分析其内容。发行机构108可经由接入控制服务器210或第三方认证器212接收消息。在操作10a，发行机构108可将呈现CPN并请求发送实体102提供口令的消息发送给发送实体102。在示例实施例中，发行机构108可请求其他认证数据，诸如对问题的响应。发送实体102接收在操作10a发送的消息并在操作11a用消息作出响应。该消息可包括口令。发行机构108接收在操作11a发送的消息并验证其与关联于CPN的数据相匹配。例如，发行机构可确定该消息是否包含与关联于CPN的口令相匹配的口令。在操作12a，发行机构108将消息与认证请求的结果一起发送给发送实体102。该消息还可包含给发送实体102浏览器的用以重定向到商家104的重定向命令。

[0085] 在操作13a，发送实体102重定向到商家104。然后，商家104查询以查看发送实体102是否成功地进行了认证。在操作14a，商家104将询问发送实体102的认证状态的消息发送给支付处理网络106。在示例实施例中，该消息可以是认证状态请求消息。

[0086] 支付处理网络106接收来自操作14a的消息。认证状态模块223可分析该消息，并且可确定发行机构108。在操作15a，认证状态模块223将询问发送实体102的认证状态的消息发送给发行机构108。在示例实施例中，该消息可以是由认证状态模块223发送的认证状态请求消息。

[0087] 发行机构108接收在操作15a发送的消息，并且可分析其内容。在操作16a，发行机

构108将包含发送实体102的认证状态的消息发送给支付处理网络106。在示例实施例中，该消息是认证状态响应消息。支付处理网络106接收在操作16a发送的消息。该消息可由认证状态模块223分析。然后，在操作17a，认证状态模块223将具有发送实体102的认证状态的消息发送给商家104。在示例实施例中，该消息是认证状态响应消息。商家104分析该消息。如果认证成功，则商家104可发起与收单机构和发行机构的支付交易、或者转账交易。在操作19a，商家104可将认证确认发送给发送实体102。

[0088] C不同的发起信道和认证信道

[0089] 图5是根据示例实施例的其中发起信道与认证信道不同的远程可变认证过程的过程流。这可描述发起和认证信道不同的情形，诸如经由web发起认证而经由SMS进行认证。其他可能的发起信道和认证信道对包括：web/移动web、SMS/IVR、USSD2/IVR、SMS/移动应用、USSD2/移动应用、CSR/IVR、IVR/移动应用、以及CSR/移动应用。为了说明起见，采用web/SMS发起和认证信道对。在示例实施例中，移动web、SMS、USSD2、IVR、移动应用、以及CSR方法可经由移动电话设备进行。

[0090] 发送实体移动电话501是发送实体102接收和发送SMS信息以与发行机构108进行认证的移动电话。发送实体计算机502是发送实体102的连接到发起认证的web的计算机。发送实体移动电话501可以是在SMS信道上通信的设备的一个实施例。发送实体计算机502可以是在web信道上通信的设备的一个实施例。

[0091] 从图3结束的地方开始，图5的过程在操作8b开始，其中商家104将消息发送给发送实体计算机502。该消息可通知发送实体102将进行带外认证，即将在不同于发起信道的信道上进行认证。该消息可经由发起信道发送。发送实体计算机502可使用从发起信道标识符导出的信息来联系。例如，发起信道标识符可描述发行机构108可通过其联系发送实体计算机502的电话号码、IP地址、或者其他数据。

[0092] 然后，在操作9b，发行机构108通过联系发送实体移动电话501来开始认证。发送实体移动电话501可根据从发起信道标识符导出的信息(诸如电话号码或IP地址)联系。例如，如果认证信道使用SMS，则发行机构108可将SMS消息经由SMS发送给发送实体移动电话501。如果认证信道使用IVR过程，则发行机构108将发起对发送实体移动电话501的呼叫。如果认证信道使用移动应用，则发行机构108可将消息经由发送实体移动电话501发送给移动应用。发行机构108可指示其准备好开始认证并且发送实体102应当对其作出响应以便于认证。

[0093] 在操作10b，发送实体移动电话501接收在操作9b发送的信息。发送实体102经由发送实体移动电话501作出响应，并且将认证请求传达给发行机构108。

[0094] 发行机构108接收在操作10b来自发送实体的移动电话501的传达。在操作11b，发行机构108将CPN传达给发送实体移动电话501并请求发送实体102提供口令或回应来进行认证。发送实体移动电话501接收操作11b的传达，并且在操作12b用口令或回应作出响应。发行机构108接收在操作12b传达的口令或回应，并验证其与关联于CPN的口令或回应相匹配。在操作13b，发行机构108将消息与认证请求的结果一起发送给发送实体移动电话501。

[0095] 操作14b、15b、16b和17b在操作9b、10b、11b、12b和13b期间和之后连续地执行和循环达预定时间量，以检查发送实体102的认证状态。在操作8b之后，商家104等待发送实体102与发行机构108进行认证。在操作14b，商家104可向支付处理网络106传达正在请求认证

状态。在示例实施例中，该传达是认证状态请求消息。支付处理网络106接收操作14b的传达，并且可在操作15b向发行机构传达正在请求认证状态。认证状态模块223可接收操作14b的传达，并向操作15b传达消息。在示例实施例中，该传达是认证状态请求消息。

[0096] 发行机构108可接收操作15b的传达。然后，在操作16b，发行机构108可将认证状态传达给支付处理网络106。认证状态可指示认证成功、失败、在进行中、或者等待来自发送实体102的响应。在示例实施例中，该传达是认证状态响应消息。商家104可接收操作17b的传达，并分析该内容。如果商家104确定认证成功，则在操作18b，商家104继续支付交易或转账，并在操作19b将认证确认发送给发送实体计算机502。如果认证不成功、在进行中、或者等待来自发送实体移动电话501的响应，则操作14b-17b循环直至预定时间段届满。

[0097] D.相同的发起信道和认证信道

[0098] 图6是根据示例实施例的其中发起信道与认证信道相同的远程可变认证过程的过程流。这可描述发起和认证信道相同的情形，诸如经由IVR发起和进行认证。图6的操作类似于图5的操作，不同之处在于，代替单独的发送实体发起设备和发送实体认证设备，只存在一个发送实体设备602。发送实体设备602可以是移动电话、计算机、或者可能接收消息并将消息发送给发行机构108的任何设备。用以联系发送实体设备602的信息可从发起信道标识符导出。例如，发起信道标识符可描述发行机构108通过其联系发送实体设备602的电子邮件地址。

[0099] 在操作8c，商家104将消息发送给发送实体设备602。该消息可以是对将进行认证的发送实体设备602的响应。

[0100] 然后，在操作9c，发行机构108通过联系发送实体设备602来开始认证。例如，如果组合信道使用SMS，则发行机构108可将SMS消息经由SMS发送给发送实体设备602。如果组合信道使用IVR过程，则发行机构108将经由电话发起对发送实体设备602的呼叫。如果组合信道使用移动应用，则发行机构108可将消息经由发送实体设备602发送给移动应用。该消息可指示发行机构准备好开始认证并对其作出响应来进行认证。在操作10c，发送实体设备602将认证请求发送给发行机构108。

[0101] 发行机构108接收在操作10c由发送实体设备602发送的消息，并分析其内容。在操作11c，发行机构108将CPN传达给发送实体设备602并请求发送实体102提供口令或回应来进行认证。发送实体设备602接收在操作11c发送的传达，并在操作12c用包括口令或回应的消息作出响应。发行机构108接收在操作12c发送的口令或回应，并验证其与关联于CPN的口令或回应相匹配。在操作13c，发行机构108将消息与认证请求的结果一起发送给发送实体设备602。

[0102] 操作14c、15c、16c和17c在操作9c、10c、11c、12c和13c期间和之后连续地执行和循环达预定时间量，以检查发送实体102的认证状态。在操作8b之后，商家104等待发送实体102与发行机构108进行认证。在操作14c，商家104将请求认证状态的消息发送给支付处理网络106。在示例实施例中，该消息是认证状态请求消息。支付处理网络106接收在操作14c发送的消息，并且可在操作15c将请求认证状态的消息发送给发行机构。在示例实施例中，该消息是认证状态请求消息。

[0103] 发行机构108可接收在操作15c发送的消息，并分析其内容。然后，在操作16c，发行机构108可将指示认证状态的消息发送给支付处理网络106。认证状态可指示认证成功、失

败、在进行中、或者等待来自发送实体102的响应。在示例实施例中，该消息是认证状态响应消息。商家104可接收在操作17c发送的消息，并分析该内容。如果商家104确定认证成功，则在操作18c，商家104继续支付交易或转账，并在操作19c将认证确认发送给发送实体设备。如果认证不成功、在进行中、或者等待来自发送实体设备602的响应，则操作14c-17c循环直至预定时间段届满。

[0104] 在发送实体成功地认证和完成图3-6中所列出的操作之后，发送实体可继续支付交易或转账。在购买交易中，发送实体在商家使用可以是信用卡形式的便携式消费类设备来购买商品或服务。消费者的便携式消费类设备可与商家处的诸如POS(销售点)终端之类的接入设备交互。例如，发送实体可携带信用卡，并且可将其刷过POS终端中的适当槽。替换地，POS终端可以是非接触式读取器，并且便携式消费类设备可以是诸如非接触式卡之类的非接触式设备。

[0105] 然后，将授权请求消息转发给收单机构。在接收到授权请求消息之后，该授权请求消息随后被发送给支付处理系统。然后，支付处理系统将授权请求消息转发给便携式消费类设备的发行机构。

[0106] 在发行机构接收到授权请求消息之后，发行机构将授权响应消息发送回支付处理系统以指示授权(还是不授权)当前交易。然后，支付处理系统将授权响应消息转发回收单机构。然后，收单机构将响应消息发送回商家。

[0107] 当商家接收到授权响应消息之后，商家处的接入设备随后可向消费者提供授权响应消息。响应消息可由POS终端显示，或者可在收据上打印出来。

[0108] 在一天结束时，正常的清算和结算过程可由交易处理系统进行。清算过程是在收单机构和发行机构之间交换金融明细以便于向消费者的帐户过帐和与消费者的结算位置对帐的过程。清算和结算可同时发生。

[0109] 本发明的各个实施例不限于上述的具体实施例。

[0110] 在另一示例实施例中，从发行机构的观点来看，认证步骤可包括：从支付处理网络接收包括主账号和认证信道标识符的消息；在认证信道标识符所描述的认证信道上接收来自发送实体的口令；针对与主账号相关联的便携式消费类设备，用口令认证发送实体；从支付处理网络接收对发送实体的认证状态的请求；以及用发送实体的认证状态对请求作出响应。

[0111] 图7是根据示例实施例的计算机装置的示图。前述系统图中的各个参与者和元件(例如，图1、2、3、4、5、6中的商家、发行机构、接入控制服务器、第三方认证器、支付处理网络等)可使用计算机装置中的任何合适数量的子系统来便于本文中所述的功能。这些子系统或组件的示例在图7中示出。图7所示的子系统经由系统总线775互连。示出了诸如打印机774、键盘778、固定盘779(或者包括计算机可读介质的其他存储器)、耦合到显示适配器782的监视器776等附加子系统。耦合到I/O(输入/输出)控制器771的外围设备和I/O设备可通过本领域已知的任何数量的手段(诸如串行端口777)连接到计算机系统。例如，串行端口777或外部接口781可用于使计算机装置连接到诸如因特网之类的广域网、鼠标输入设备、或者扫描仪。经由系统总线的互连可允许中央处理器773与每一子系统通信，并控制来自系统存储器772或固定盘779的指令的执行，以及子系统之间的信息交换。系统存储器772和/或固定盘779可体现为计算机可读介质。

[0112] 本申请中所述的软件组件或功能可被实现为由一个或多个处理器使用例如常规或面向对象技术、使用任何合适的计算机语言(举例而言,诸如Java、C++、或Perl)执行的软件代码。软件代码可作为一系列指令或命令被存储在诸如随机存取存储器(RAM)、只读存储器(ROM)、磁介质(诸如硬驱动器或软盘)、或者光学介质(诸如CD-ROM)之类的计算机可读介质上。任何这种计算机可读介质还可驻留在单个计算装置上或其内部,并且可存在于系统或网络内的不同计算装置上或其内部。

[0113] 本发明可以软件或硬件、或者两者的组合中的控制逻辑的形式来实现。该控制逻辑可作为多个指令被储存在信息储存介质中,这些指令适于引导信息处理设备执行在本发明的各个实施例中所公开的一系列步骤。基于本文中所提供的公开和教义,本领域普通技术人员应当理解实现本发明的其他发送和/或方法。

[0114] 在各个实施例中的,本文中所示的任一实体可体现为执行所公开的功能和步骤的任一个或全部的计算机。

[0115] 对“一”、“一个”或“该”的任何叙述旨在表示“一个或多个”,除非具体地指示了相反含义。

[0116] 以上描述是说明性而非限制性的。在审阅本公开之后,本发明的许多变体对本领域技术人员而言将变得显而易见。因此,本发明的范围不应参考以上描述来确定,相反应当参考所附权利要求及其全部范围或等效方案来确定。

[0117] 特定实施例在本文中被描述为包括逻辑、或者大量组件、模块或机构。模块可构成软件模块(例如,在机器可读介质上或在传输信号中所体现的代码)或硬件模块。硬件模块是能够执行特定操作的有形单元,并且可以特定方式配置或排列。在示例实施例中,一个或多个计算机系统(例如,独立的客户机或服务器计算机系统)、或者计算机系统的一个或多个硬件模块(例如,一个处理器或一组处理器)可由作为操作以执行如本文中所述的特定操作的硬件模块的软件(例如,应用或应用部分)配置。

[0118] 在各个实施例中,硬件模块可机械地实现或电实现。例如,硬件模块可包括永久配置以执行特定操作的专用电路或逻辑(例如,诸如现场可编程门阵列(PFGA)或专用集成电路(ASIC)之间的专用处理器)。硬件模块还可包括由软件临时配置以执行特定操作的可编程逻辑或电路(例如,涵盖在通用处理器或其他可编程处理器内的)。应当理解,在专用和永久配置的电路中、还是在临时配置的电路(例如,由软件配置的)中机械地实现硬件模块的判定可由成本和时间考虑驱动。

[0119] 因此,术语“硬件模块”应当理解为涵盖作为物理地构造、永久地配置(例如,硬接线的)、或临时地配置(例如,经编程的)从而以特定方式操作和/或执行本文中所述的特定操作的实体的有形实体。考虑到其中临时配置(例如,经编程的)硬件模块的各个实施例,每一硬件模块不需要在任一时间实例配置或例示。例如,在硬件模块包括使用软件配置的通用处理器的地方,通用处理器可在不同时刻被配置为相应的不同硬件模块。因此,软件可配置处理器来例如在一个时间实例构成特定的硬件模块、而在不同时间实例构成不同的硬件模块。

[0120] 硬件模块可向其他硬件模块提供信息,并从其他硬件模块接收信息。因此,所述的硬件模块可被认为是通信地耦合。在多个这种硬件模块同时存在的地方,通信可通过连接硬件模块的信号传输(例如,在适当的电路和总线上)来实现。在其中多个硬件模块在不同

时刻配置或例示的各个实施例中，这些硬件模块之间的通信可例如通过在多个硬件模块可访问的存储器结构中存储和检索信息来实现。例如，一个硬件模块可执行操作，并将该操作的输出存储在其通信地耦合的存储器设备中。然后，另一硬件模块可在稍后的时刻访问存储器设备以检索和处理所存储的输出。硬件模块还可发起与输入或输出设备的通信，并且可对资源(例如，信息的收集)进行操作。

[0121] 本文中所述的示例方法的各个操作可至少部分地由临时配置(例如，由软件)或永久配置以执行相关操作的一个或多个处理器执行。无论是临时配置还是永久配置，这些处理器都可构成操作以执行一个或多个操作或功能的处理器实现的模块。在一些示例实施例中，本文中所指的模块可包括处理器实现的模块。

[0122] 类似地，本文中所述的方法可以是至少部分由处理器实现的。例如，方法的至少一些操作可由一个或多个处理器或处理器实现的模块执行。特定操作的性能可分布在一个或多个处理器之间，不仅驻留在单个机器内，而且跨大量机器部署。在一些示例实施例中，一个或多个处理器可位于单个位置(例如，在家庭环境、办公室环境、或服务器场内)，而在其他实施例中，处理器可跨多个位置分布。

[0123] 一个或多个处理器还可操作以支持“云计算”环境或“作为服务的软件(SaaS)”中的相关操作的性能。例如，至少一些操作可由一组计算机(例如，包括处理器的机器的示例)执行，这些操作可经由网络(例如，因特网)、以及经由一个或多个适当的接口(例如，应用程序接口(API))访问。

[0124] 远程可变认证处理系统的各个实施例提供优于现有系统的若干优点。远程可变认证处理系统允许发送实体在不公开诸如信用卡号码之类的任何敏感信息的情况下认证。远程可变认证处理还允许发送实体选择希望通过其认证的认证信道，并且根据所选的认证信道提供单独的过程。这增大了认证的价值，因为其还可验证用户拥有特定设备。该处理还可增加认证系统的效用，因为其允许用户使用多种方法认证。同样，可确定或实施兼容的发起信道和认证信道。

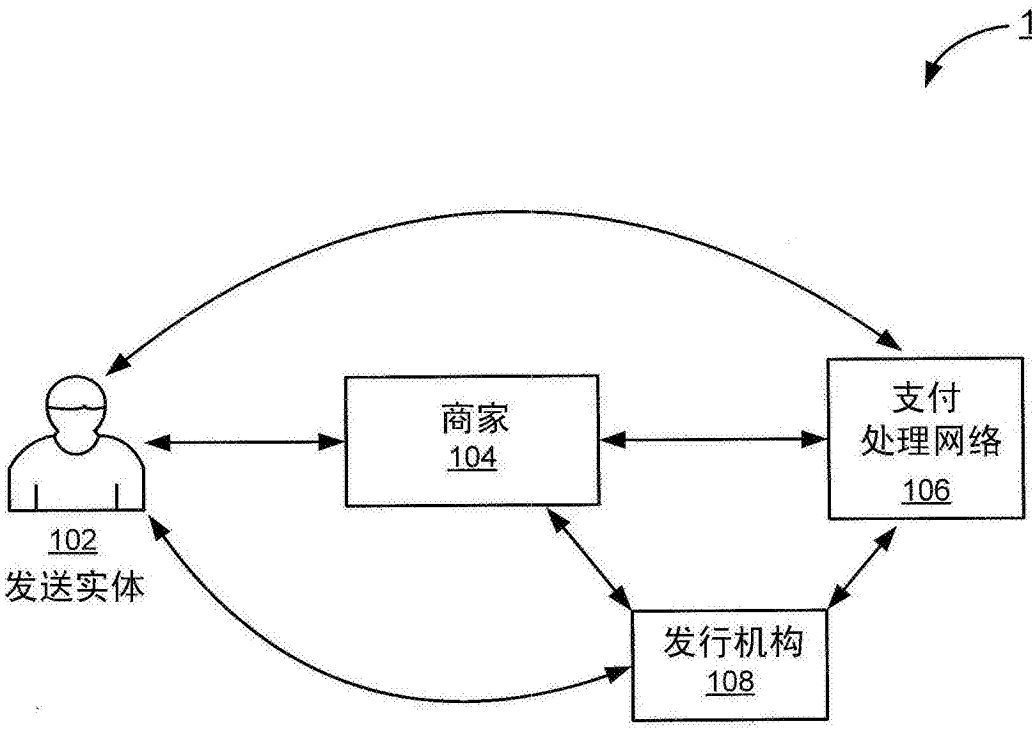


图1

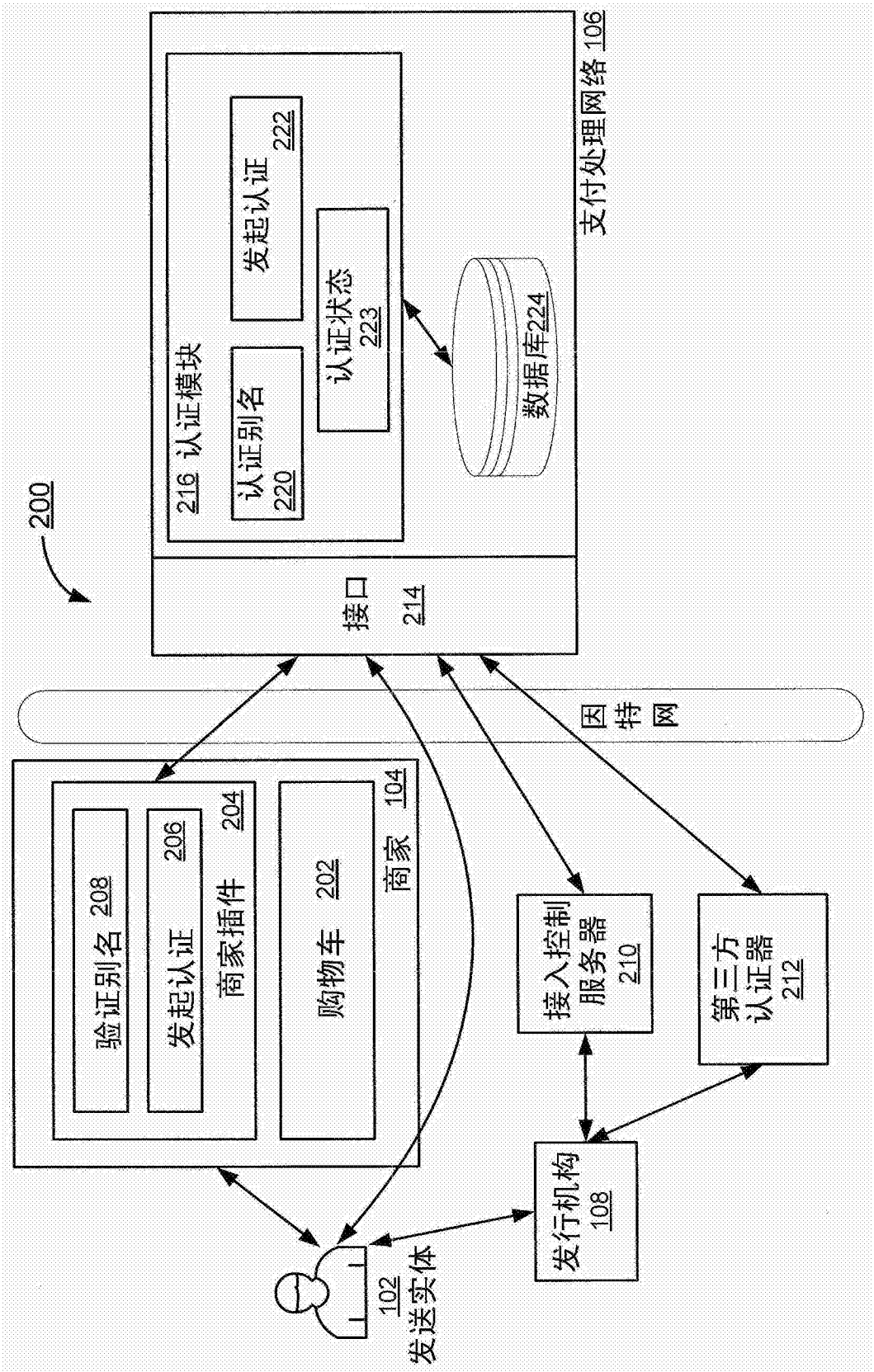

200
支付处理网络 106
216 认证模块
发起认证 222
认证别名 220
认证状态 223
数据库224
接口 214
因特网
商家 104
验证别名 208
发起认证 206
商家插件 204
购物车 202
接入控制服务器 210
第三方认证器 212
发行机构 108
102 发送实体

图2

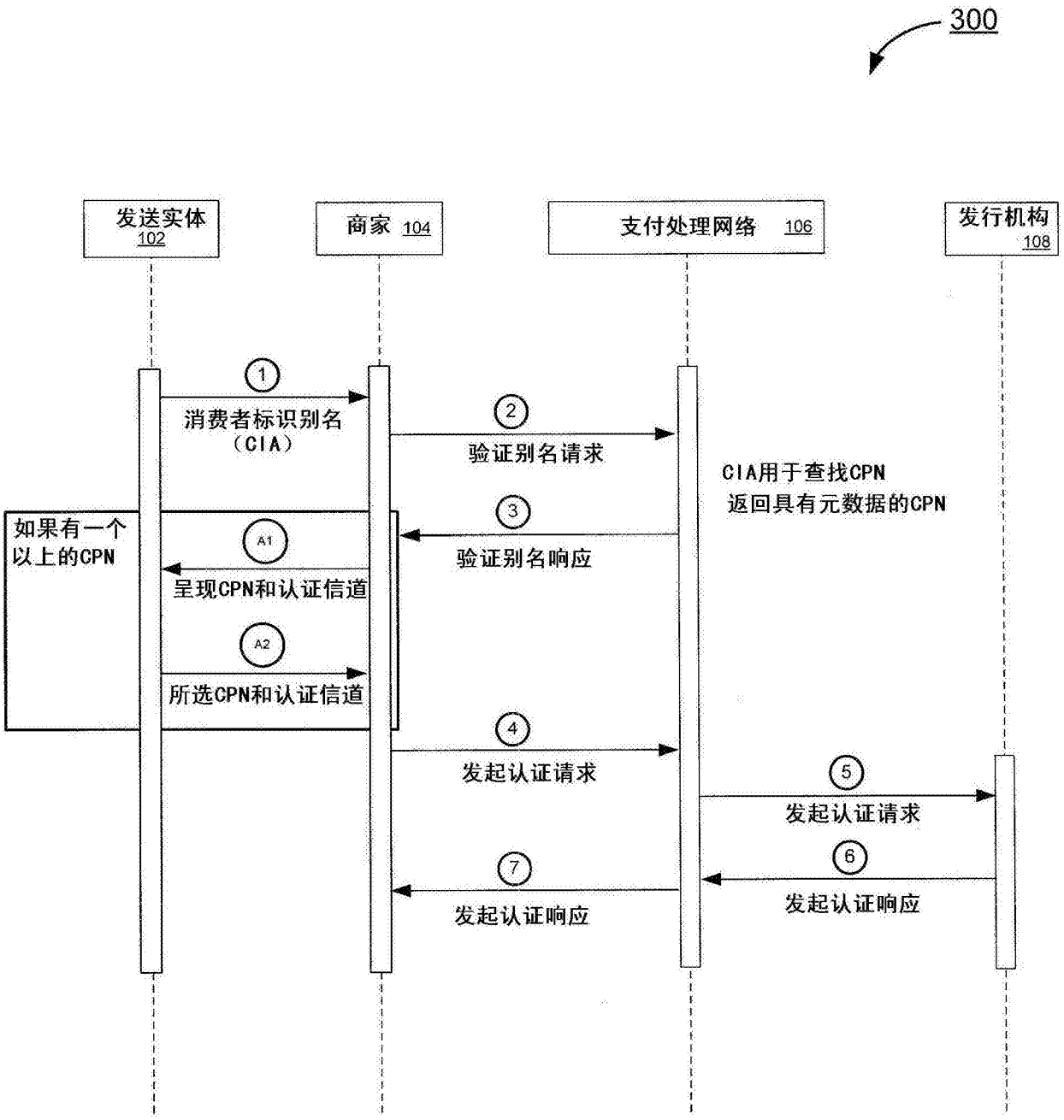

300
发送实体
102
商家 104
支付处理网络 106
发行机构
108
1
消费者标识别名
（CIA）
2
验证别名请求
CIA用于查找CPN
返回具有元数据的CPN
3
验证别名响应
如果有一个
以上的CPN
A1
呈现CPN和认证信道
A2
所选CPN和认证信道
4
发起认证请求
5
发起认证请求
6
发起认证响应
7
发起认证响应

图3

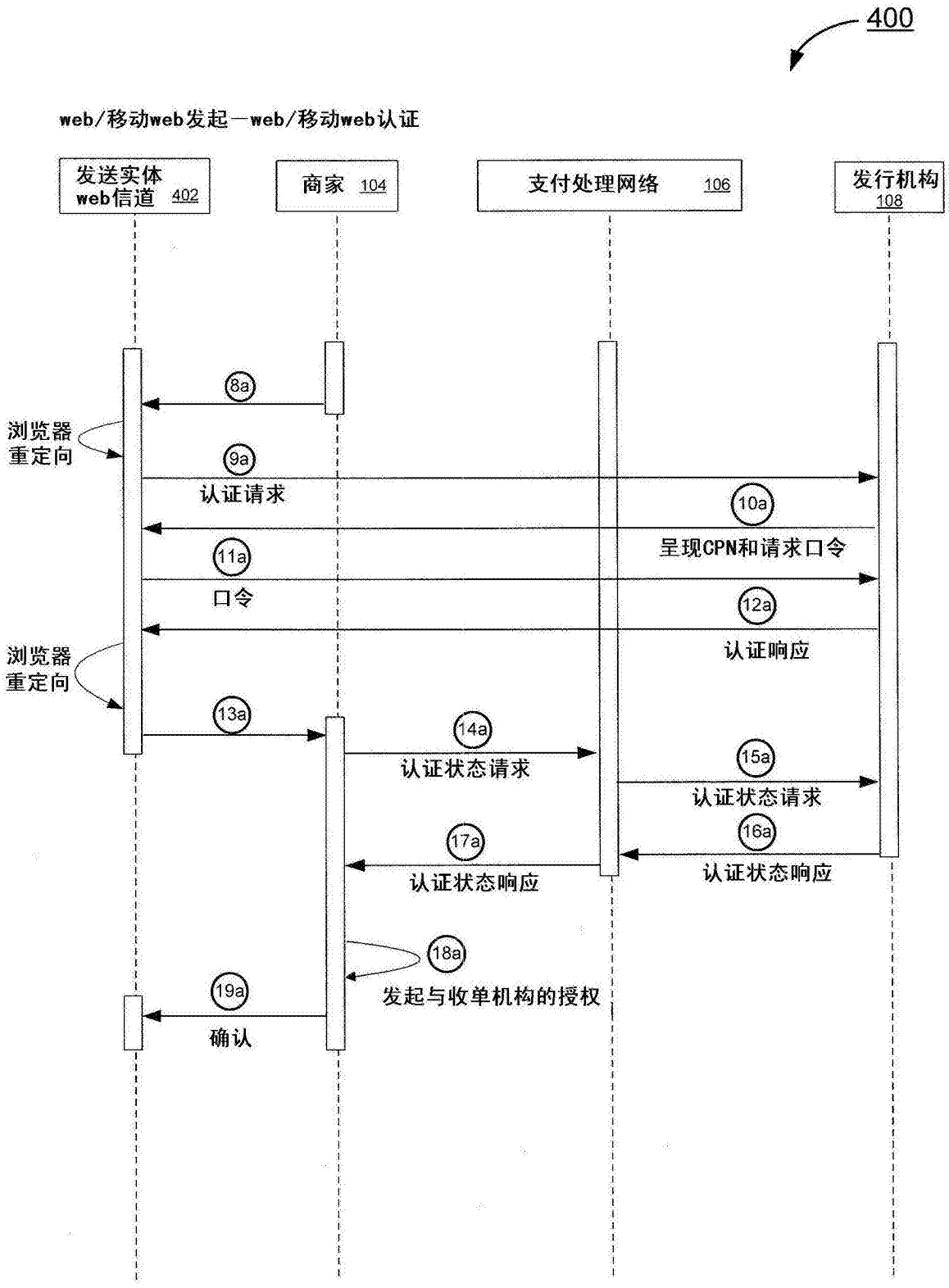

400
web/移动web发起—web/移动web认证
发送实体 web信道 402
商家 104
支付处理网络 106
发行机构 108
8a
浏览器 重定向
9a
认证请求
10a
呈现CPN和请求口令
11a
口令
12a
认证响应
浏览器 重定向
13a
14a
认证状态请求
15a
认证状态请求
16a
认证状态响应
17a
认证状态响应
18a
发起与收单机构的授权
19a
确认

图4

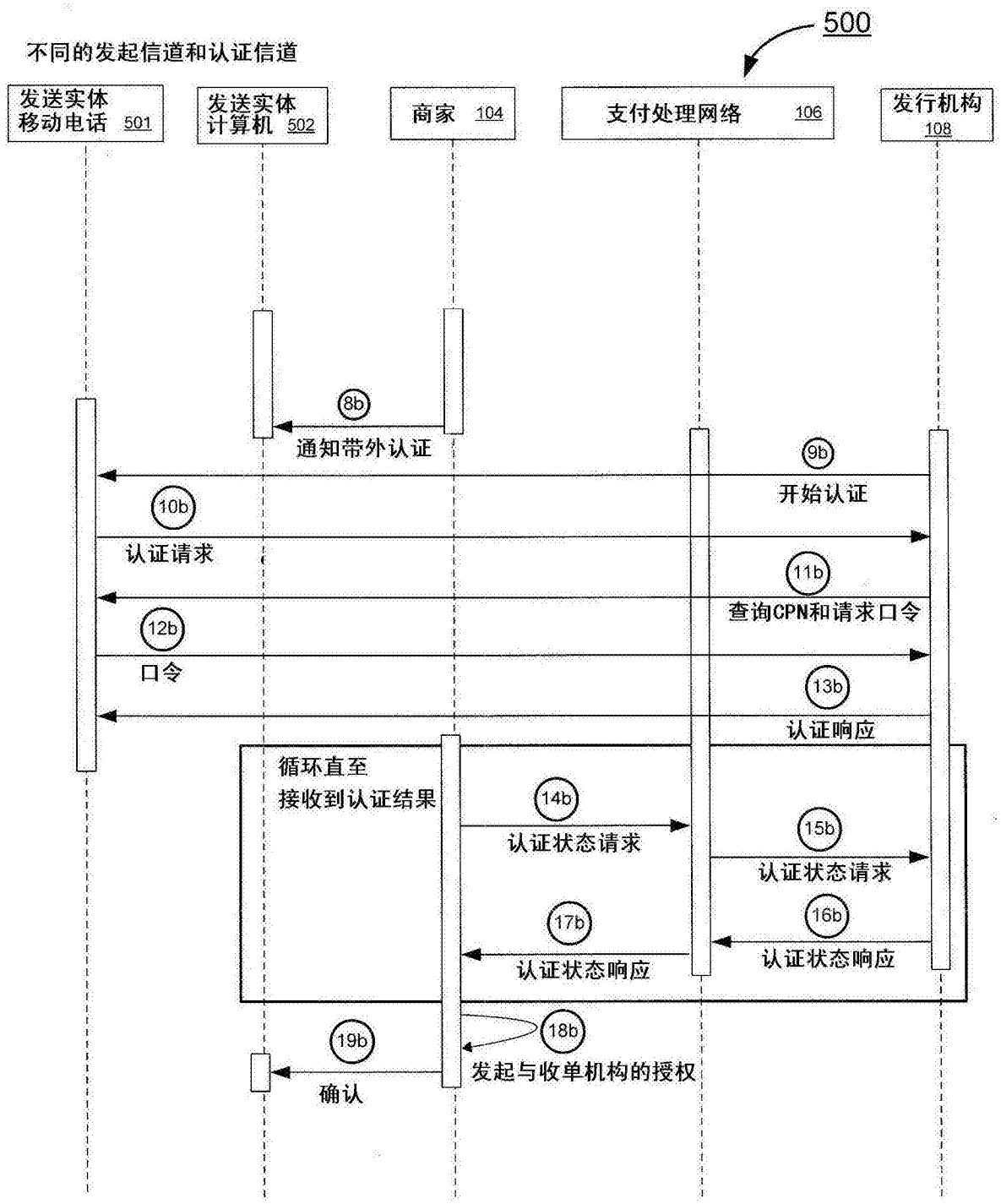

500
不同的发起信道和认证信道
发送实体
移动电话 501
发送实体
计算机 502
商家 104
支付处理网络 106
发行机构
108
8b
通知带外认证
9b
开始认证
10b
认证请求
11b
查询CPN和请求口令
12b
口令
13b
认证响应
循环直至
接收到认证结果
14b
认证状态请求
15b
认证状态请求
16b
认证状态响应
17b
认证状态响应
18b
发起与收单机构的授权
19b
确认

图5

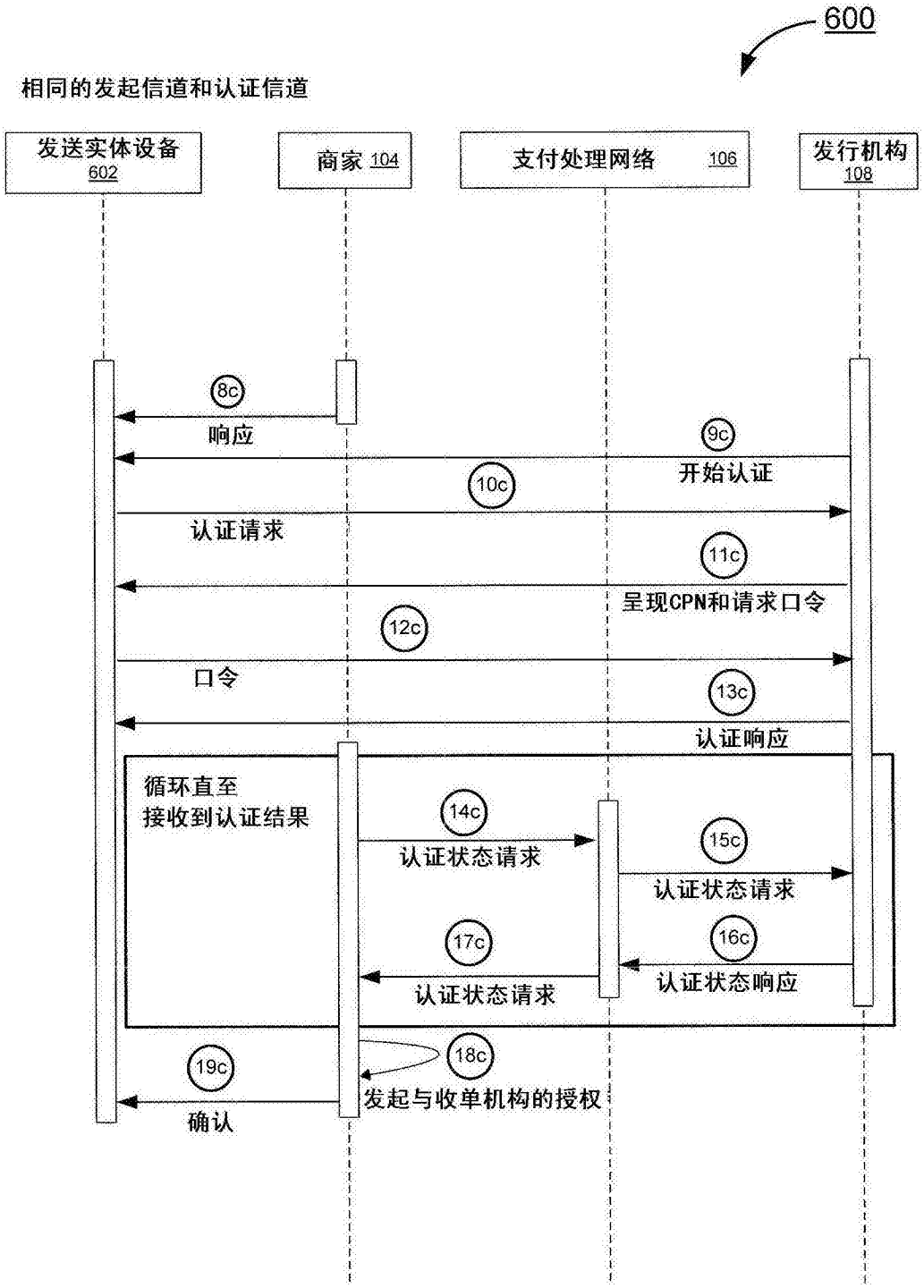

600
相同的发起信道和认证信道
发送实体设备 602
商家 104
支付处理网络 106
发行机构 108
8c
响应
9c
开始认证
10c
认证请求
11c
呈现CPN和请求口令
12c
口令
13c
认证响应
循环直至
接收到认证结果
14c
认证状态请求
15c
认证状态请求
16c
认证状态响应
17c
认证状态请求
18c
发起与收单机构的授权
19c
确认

图6

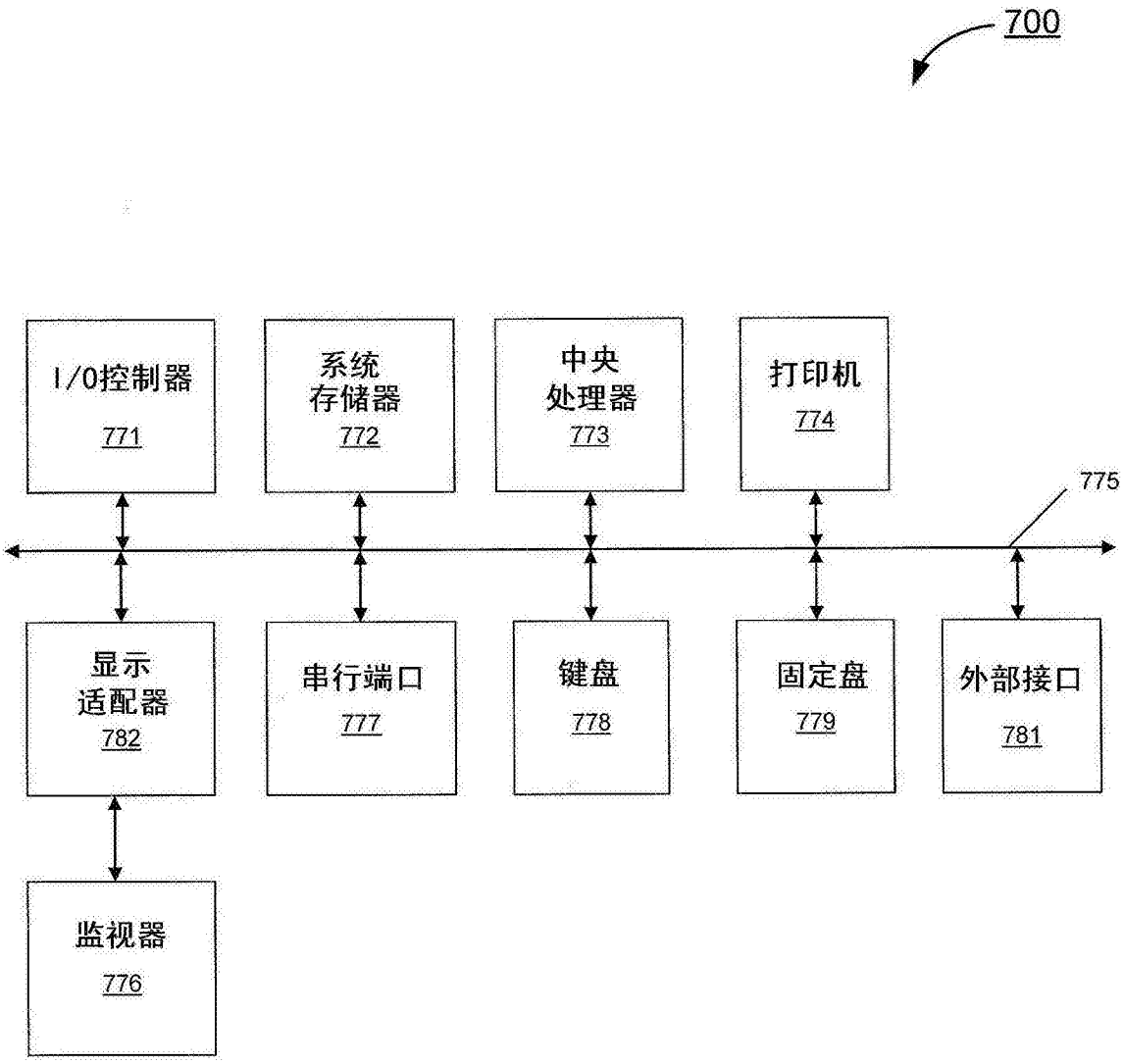

700
I/O控制器
771
系统
存储器
772
中央
处理器
773
打印机
774
775
显示
适配器
782
串行端口
777
键盘
778
固定盘
779
外部接口
781
监视器
776

图7