(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110633987 B
(45)授权公告日 2023.06.27

(21)申请号 201910548622.0

(22)申请日 2019.06.24

(65)同一申请的已公布的文献号
申请公布号 CN 110633987 A

(43)申请公布日 2019.12.31

(30)优先权数据
62/688,546 2018.06.22 US

(73)专利权人 万事达卡国际公司
地址 美国纽约

(72)发明人 J·S·戈塞特 R·A·埃德勒
R·S·伊耶 B·皮尔 N·古拉蒂
P·贝克 C·J·默茨
F·J·弗洛里

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 周衡威

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

(56)对比文件
CN 107533705 A,2018.01.02
CN 1407426 A,2003.04.02

审查员 孙丹

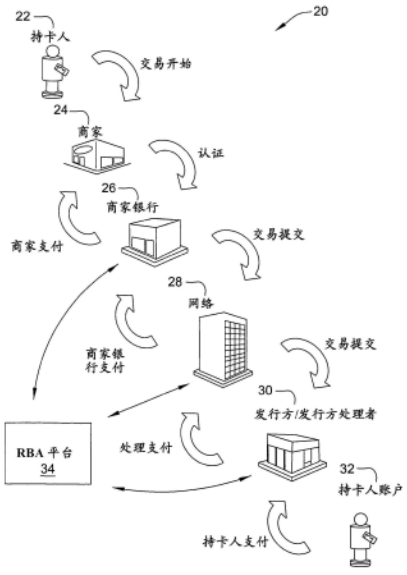
权利要求书4页 说明书36页 附图13页

(54)发明名称

在受监管环境中认证在线用户的系统和方法

(57)摘要

公开了在受监管环境中认证在线用户的系统和方法。用于认证交易中的在线用户而不使用强消费者认证(SCA)的认证平台包括接收涉及受监管的市场的交易的认证请求消息(包括认证数据和交易价值)、从认证请求消息提取认证数据、生成基于风险的认证(RBA)结果数据、通过相对于由监管实体建立的风险阈值评估风险分数确定交易中的欺诈风险满足风险阈值、确定交易价值低于监管实体设定的交易限制(该交易限制标识阈值交易价值,对于满足风险阈值的交易,在低于阈值交易价值的情况下强消费者认证可以被避免),以及基于满足风险阈值并且低于交易限制而发送认证响应消息,从而在没有对交易执行强消费者认证的情况下认证交易。



CN 110633987 B

1.一种用于在不使用强消费者认证(SCA)的情况下对交易中的在线用户进行认证的认证平台,所述认证平台包括:

存储器设备;以及

耦合到所述存储器设备的至少一个处理器,所述至少一个处理器被编程为:

接收用于交易的认证请求消息,所述认证请求消息包括认证数据和交易价值;

从所述认证请求消息中提取所述认证数据;

至少部分地基于所提取的所述认证数据生成基于风险的认证(RBA)结果数据,所述基于风险的认证(RBA)结果数据包括用于所述交易的风险分数;

基于所述认证数据确定所述交易涉及在条件强消费者认证(SCA)下操作的市场,其中操作所述市场的监管实体强制要求某些交易需要强消费者认证;

向操作所述市场的监管实体显示图形用户界面GUI控制面板,其中显示GUI控制面板包括:

从所述监管实体接收i)风险阈值和ii)交易限额,其中不强制要求满足所述风险阈值和所述交易限额两者的交易利用强消费者认证(SCA)进行认证,并且其中强制要求不满足所述风险阈值和所述交易限额中的至少一个的交易利用强消费者认证(SCA)进行认证;

生成第一历史欺诈数据,其中所述第一历史欺诈数据指示基于接收到的风险阈值和交易限额未被强制要求进行认证的以前进行的交易中的欺诈程度;

生成第二历史欺诈数据,其中所述第二历史欺诈数据指示基于接收到的风险阈值和交易限额被强制要求进行认证的以前进行的交易中的欺诈程度;以及

在GUI控制面板上显示所述第一历史欺诈数据和所述第二历史欺诈数据;

将所述基于风险的认证(RBA)结果数据与包括所述风险阈值和所述交易限额的认证建档进行比较;

基于所述比较,通过相对于由所述监管实体建立的风险阈值评估所述风险分数,确定所述交易中的欺诈风险满足所述风险阈值;

基于所述比较,确定所述交易价值低于由所述监管实体设定的交易限制,所述交易限制标识阈值交易价值,其中,对于满足所述风险阈值的交易,在低于所述阈值交易价值的情况下强消费者认证可以被避免;以及

基于所确定的欺诈风险满足所述风险阈值并且进一步基于所确定的交易额低于所述交易限制,发送认证响应消息,所述认证响应消息在没有对所述交易执行强消费者认证的情况下对所述交易进行认证。

2.根据权利要求1所述的认证平台,所述处理器还被配置为:

生成与所述交易相关联的增强的认证请求消息,所述增强的认证请求消息包括指示所述交易没有被强制要求强消费者认证的数据;以及

将所述增强的认证请求消息发送给接入控制服务器ACS。

3.根据权利要求2所述的认证平台,所述处理器还被配置为:

生成与另一个交易相关联的另一个增强的认证请求消息,所述另一个增强的认证请求消息包括指示该交易被强制要求强消费者认证的数据;以及

将所述另一个增强的认证请求消息发送给接入控制服务器,所指示的强制要求使得所述接入控制服务器针对所述另一个交易发起强消费者认证(SCA)。

4.根据权利要求1所述的认证平台,其中,所述第一历史欺诈数据包括基于接收到的风险阈值和交易限额未被强制要求进行认证的先前进行的交易的批准率,并且其中,和所述第二历史欺诈数据包括基于接收到的风险阈值和交易限额被强制要求进行认证的先前进行的交易的批准率。

5.根据权利要求1所述的认证平台,其中,所述基于风险的认证(RBA)结果数据还包括至少一个原因代码,所述至少一个原因代码指示影响了所生成的风险分数的至少一个因素。

6.根据权利要求1所述的认证平台,所述处理器还被配置为:

从所述监管实体接收:i)更新的风险阈值和ii)更新的交易限额;以及

基于历史交易数据估计如果交易基于所述更新的风险阈值和所述更新的交易限额被强制要求利用强消费者认证(SCA)进行认证的欺诈程度;以及

更新GUI仪表板以包括估计的欺诈程度。

7.一种用于在不使用强消费者认证(SCA)的情况下对交易中的在线用户进行认证的计算机实现的方法,所述方法被实现在计算设备上,所述计算设备包括耦合到至少一个处理器的存储器设备,并且所述方法包括:

接收用于交易的认证请求消息,所述交易涉及受监管实体监管的市场,所述认证请求消息包括认证数据和交易价值;

从所述认证请求消息中提取所述认证数据;

至少部分地基于所提取的所述认证数据生成基于风险的认证(RBA)结果数据,所述基于风险的认证(RBA)结果数据包括用于所述交易的风险分数;

基于所述认证数据确定所述交易涉及在条件强消费者认证(SCA)下操作的市场,其中操作所述市场的监管实体强制要求某些交易需要强消费者认证;

向操作所述市场的监管实体显示图形用户界面GUI控制面板,其中显示GUI控制面板包括:

从所述监管机构接收i)风险阈值和ii)交易限额,其中不强制要求满足所述风险阈值和所述交易限额两者的交易利用强消费者认证(SCA)进行认证,并且其中强制要求不满足所述风险阈值和所述交易限额中的至少一个的交易利用强消费者认证(SCA)进行认证;

生成第一历史欺诈数据,其中所述第一历史欺诈数据指示基于接收到的风险阈值和交易限额未被强制要求进行认证的以前进行的交易中的欺诈程度;

生成第二历史欺诈数据,其中所述第二历史欺诈数据指示根据收到的风险阈值和交易限额被强制要求进行认证的以前进行的交易中的欺诈程度;以及

在GUI控制面板上显示所述第一历史欺诈数据和所述第二历史欺诈数据;

将所述基于风险的认证(RBA)结果数据与包括所述风险阈值和所述交易限额的认证建档进行比较;

基于所述比较,通过相对于由所述监管实体建立的风险阈值评估所述风险分数,确定所述交易中的欺诈风险满足所述风险阈值;

基于所述比较,确定所述交易价值低于由所述监管实体设定的交易限制,所述交易限制标识阈值交易价值,其中,对于满足所述风险阈值的交易,在低于所述阈值交易价值的情况下强消费者认证可以被避免;以及

基于所确定的欺诈风险满足所述风险阈值并且进一步基于所确定的交易额低于所述交易限制,发送认证响应消息,所述认证响应消息在没有对所述交易执行强消费者认证的情况下对所述交易进行认证。

8.根据权利要求7所述的方法,还包括:

生成与所述交易相关联的增强的认证请求消息,所述增强的认证请求消息包括指示所述交易没有被强制要求强消费者认证的数据;以及

将所述增强的认证请求消息发送给接入控制服务器ACS。

9.根据权利要求8所述的方法,还包括:

生成与另一个交易相关联的另一个增强的认证请求消息,所述另一个增强的认证请求消息包括指示该交易被强制要求强消费者认证的数据;以及

将所述另一个增强的认证请求消息发送给接入控制服务器,所指示的强制要求使得所述接入控制服务器针对所述另一个交易发起强消费者认证(SCA)。

10.根据权利要求7所述的方法,其中,所述第一历史欺诈数据和所述第二历史欺诈数据中的一个或多个包括欺诈的基点和批准率。

11.根据权利要求7所述的方法,其中,所述基于风险的认证(RBA)结果数据还包括至少一个原因代码,所述至少一个原因代码指示影响了所生成的风险分数的至少一个因素。

12.至少一个非暂态计算机可读存储介质,具有实现在其上的计算机可执行指令以用于在不使用强消费者认证(SCA)的情况下对交易中的在线用户进行认证,其中,所述计算机可执行指令当由至少一个处理器执行时使得所述至少一个处理器执行以下操作:

接收用于交易的认证请求消息,所述交易涉及受监管实体监管的市场,所述认证请求消息包括认证数据和交易价值;

从所述认证请求消息中提取所述认证数据;

至少部分地基于所提取的所述认证数据生成基于风险的认证(RBA)结果数据,所述基于风险的认证(RBA)结果数据包括用于所述交易的风险分数;

基于所述认证数据确定所述交易涉及在条件强消费者认证(SCA)下操作的市场,其中操作所述市场的监管实体强制要求某些交易需要强消费者认证;

向操作所述市场的监管实体显示图形用户界面GUI控制面板,其中显示GUI控制面板包括:

从所述监管机构接收i)风险阈值和ii)交易限额,其中不强制要求满足所述风险阈值和所述交易限额两者的交易利用强消费者认证(SCA)进行认证,并且其中强制要求不满足所述风险阈值和所述交易限额中的至少一个的交易利用强消费者认证(SCA)进行认证;

生成第一历史欺诈数据,其中所述第一历史欺诈数据指示基于接收到的风险阈值和交易限额未被强制要求进行认证的以前进行的交易中的欺诈程度;

生成第二历史欺诈数据,其中所述第二历史欺诈数据指示根据收到的风险阈值和交易限额被强制要求进行认证的以前进行的交易中的欺诈程度;以及

在GUI控制面板上显示所述第一历史欺诈数据和所述第二历史欺诈数据;

将所述基于风险的认证(RBA)结果数据与包括所述风险阈值和所述交易限额的认证建档进行比较;

基于所述比较,通过相对于由所述监管实体建立的风险阈值评估所述风险分数,确定

所述交易中的欺诈风险满足所述风险阈值;

基于所述比较,确定所述交易价值低于由所述监管实体设定的交易限制,所述交易限制标识阈值交易价值,其中,对于满足所述风险阈值的交易,在低于所述阈值交易价值的情况下强消费者认证可以被避免;以及

基于所确定的欺诈风险满足所述风险阈值并且进一步基于所确定的交易额低于所述交易限制,发送认证响应消息,所述认证响应消息在没有对所述交易执行强消费者认证的情况下对所述交易进行认证。

13.根据权利要求12所述的计算机可读存储介质,所述计算机可执行指令还使得所述至少一个处理器执行以下操作:

生成与所述交易相关联的增强的认证请求消息,所述增强的认证请求消息包括指示所述交易没有被强制要求强消费者认证的数据;以及

将所述增强的认证请求消息发送给接入控制服务器ACS。

14.根据权利要求13所述的计算机可读存储介质,所述计算机可执行指令还使得所述至少一个处理器执行以下操作:

生成与另一个交易相关联的另一个增强的认证请求消息,所述另一个增强的认证请求消息包括指示该交易被强制要求强消费者认证的数据;以及

将所述另一个增强的认证请求消息发送给接入控制服务器,所指示的强制要求使得所述接入控制服务器针对所述另一个交易发起强消费者认证(SCA)。

15.根据权利要求12所述的计算机可读存储介质,其中,所述第一历史欺诈数据和所述第二历史欺诈数据中的一个或多个包括欺诈的基点和批准率。

在受监管环境中认证在线用户的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2018年6月22日提交的标题为“SYSTEMS AND METHODS FOR AUTHENTICATING ONLINE USERS”的美国临时申请No.62/688,528、于2018年6月22日提交的标题为“SYSTEMS AND METHODS FOR AUTHENTICATING ONLINE USERS WITH AN ACCESS CONTROL SERVER”的美国临时申请No.62/688,529、于2018年6月22日提交的标题为“SYSTEMS AND METHODS FOR AUTHENTICATING ONLINE USERS IN REGULATED ENVIRONMENTS”的美国临时申请No.62/688,546,以及于2018年6月22日提交的标题为“SYSTEMS AND METHODS FOR AUTHENTICATING ONLINE USERS”的美国临时申请No.62/688,532的优先权,这些申请的全部内容和公开通过引用整体并入本文。

技术领域

[0003] 本申请一般而言涉及通过电子网络认证在线用户,更具体地,涉及使用基于风险的认证在受监管环境中认证在线用户。

背景技术

[0004] 通过电子支付网络进行的交易呈指数级增长。对于卡不存在的交易(例如,消费者实际上不向商家提供支付卡的交易),欺诈明显更高。因此,对于这种交易,通常实施认证程序以验证声称的持卡人事实上是实际或合法的持卡人。

[0005] 在至少一些已知的认证系统中,发行了用于交易的支付卡的银行(称为发行方)与用于认证服务的接入控制服务器(ACS)签订合同。具体地,ACS分析与交易相关联的数据中的至少一些数据、确定声称的持卡人是否可能事实上是实际或合法的持卡人、并向发行方报告该确定。

[0006] 一些认证系统还可以针对某些交易实现强消费者认证(SCA)(或仅“强认证”)。例如,发行银行可以坚持在在线交易期间(例如,使用用户名和密码、或通过SMS文本消息)认证消费者。这些工具可以帮助发行方验证身份并认证持卡人,但它们也可能增加对持卡人的阻力,这有时会导致交易被放弃。这可能导致商家和底层支付卡网络的损失。此外,诸如密码之类的一些SCA方法可能不如其他方法可信,这可能导致交易风险增加。

[0007] 在一些市场中,监管者可能对数字交易要求SCA。例如,印度中央银行——印度储备银行(RBI)要求所有数字交易都使用SCA进行认证。虽然这些法规减少了印度的欺诈行为,但在结账时它们会产生相当大的阻力。持卡人因不得不提供密码或超时交易而感到沮丧,并且当持卡人因其沮丧而放弃交易时,商家将感到不满。

[0008] 因此,期望具有计算机实现的认证平台,其能够提供在其中可以在没有SCA的情况下认证一些交易的网络。

发明内容

[0009] 在一个方面中,提供了一种用于认证交易中的在线用户而不使用强消费者认证

(SCA)的认证平台。该认证平台包括存储器设备以及耦合到存储器设备的至少一个处理器。该认证平台接收用于交易的认证请求消息,该交易涉及受监管实体监管的市场。该认证请求消息包括认证数据和交易价值。该认证平台还从认证请求消息中提取认证数据。该认证平台进一步至少部分地基于所提取的认证数据生成基于风险的认证(risk-based authentication,RBA)结果数据,该RBA结果数据包括用于该交易的风险分数。该认证平台还通过相对于由监管实体建立的风险阈值评估风险分数,确定交易中的欺诈风险满足该风险阈值。该认证平台进一步确定交易价值低于由监管实体设定的交易限制。该交易限制标识阈值交易价值,其中,对于满足风险阈值的交易,在低于阈值交易价值的情况下强消费者认证可以被避免。该认证平台还基于所确定的欺诈风险满足风险阈值并且进一步基于所确定的交易额低于交易限制而发送认证响应消息,该认证响应消息在没有对交易执行强消费者认证的情况下对交易进行认证。

[0010] 在另一个方面中,提供了一种用于认证交易中的在线用户而不使用强消费者认证(SCA)的计算机实现的方法。该方法被实现在计算设备上,该计算设备包括耦合到至少一个处理器的存储器设备。该方法包括接收用于交易的认证请求消息,该交易涉及受监管实体监管的市场。该认证请求消息包括认证数据和交易价值。该方法还包括从该认证请求消息中提取该认证数据。该方法进一步包括至少部分地基于所提取的认证数据生成基于风险的认证(RBA)结果数据,该RBA结果数据包括用于该交易的风险分数。该方法还包括通过相对于由该监管实体建立的风险阈值评估该风险分数,确定该交易中的欺诈风险满足该风险阈值。该方法进一步包括确定该交易价值低于由该监管实体设定的交易限制。该交易限制标识阈值交易价值,其中,对于满足该风险阈值的交易,在低于该阈值交易价值的情况下强消费者认证可以被避免。该方法还包括基于所确定的欺诈风险满足该风险阈值并且进一步基于所确定的交易额低于该交易限制而发送认证响应消息,该认证响应消息在没有对该交易执行强消费者认证的情况下对该交易进行认证。

[0011] 在还有的方面,提供了至少一个非暂态计算机可读存储介质,具有实现在其上的计算机可执行指令以用于认证交易中的在线用户而不使用强消费者认证(SCA)。所述计算机可执行指令当由至少一个处理器执行时使得所述至少一个处理器接收用于交易的认证请求消息,该交易涉及受监管实体监管的市场,该认证请求消息包括认证数据和交易价值。所述计算机可执行指令还使得所述至少一个处理器从认证请求消息中提取认证数据。所述计算机可执行指令还使得所述至少一个处理器至少部分地基于所提取的认证数据生成RBA结果数据,该RBA结果数据包括用于该交易的风险分数。所述计算机可执行指令还使得所述至少一个处理器通过相对于由监管实体建立的风险阈值评估该风险分数,确定该交易中的欺诈风险满足风险阈值。所述计算机可执行指令还使得所述至少一个处理器确定该交易价值低于由该监管实体设定的交易限制。该交易限制标识阈值交易价值,其中,对于满足该风险阈值的交易,在低于该阈值交易价值的情况下强消费者认证可以被避免。所述计算机可执行指令还使得所述至少一个处理器基于所确定的欺诈风险满足该风险阈值并且进一步基于所确定的交易额低于该交易限制,发送认证响应消息,该认证响应消息在没有对该交易执行强消费者认证的情况下对该交易进行认证。

附图说明

[0012] 图1-12示出了本文描述的方法和系统的示例实施例。

[0013] 图1是示出根据本公开的一个实施例的与多方支付卡系统通信以用于处理支付交易的示例RBA平台的示意图。

[0014] 图2是根据本公开的一个示例实施例的用于处理支付交易的计算机系统的示例实施例的扩展框图，该计算机系统包括服务器系统。

[0015] 图3示出了诸如图2中所示的服务器系统的服务器系统的示例配置。

[0016] 图4示出了图2中所示的客户端系统的示例配置。

[0017] 图5是示出示例认证系统中的交易流程的示意图。

[0018] 图6是示出另一个示例认证系统中的交易流程的示意图。

[0019] 图7是用于代表接入控制服务器(ACS)认证用户的示例方法的流程图。

[0020] 图8是用于认证在线用户的另一示例方法的数据流图。

[0021] 图9是用于认证在线用户的另一示例方法的流程图。

[0022] 图10是用于代表ACS认证在线用户的另一示例方法的流程图。

[0023] 图11A和11B是说明涉及与受监管的市场相关联的交易的条件性SCA评估的附加示例实施例的泳道图。

[0024] 图12是用于认证在线用户并用于增加批准、减少欺诈和改善消费者体验的另一示例高级认证过程的流程图。

[0025] 尽管各种实施例的特定特征可能在一些附图中示出而在其他附图中未示出，但这仅是为了方便。可以结合任何其他附图的任何特征来引用和/或要求任何附图的任何特征。

具体实施方式

[0026] 本文描述的系统和方法涉及受监管的市场中的在线用户的“有条件的”强消费者认证。启用基于风险的认证(启用RBA的)目录服务器存储认证简档，该认证简档包括用于执行和路由认证请求的规则。启用RBA的目录服务器接收涉及由监管实体监管的市场的交易的认证请求消息。该认证请求消息包括认证数据和交易价值。启用RBA的目录服务器从认证请求消息中提取认证数据。启用RBA的目录服务器基于提取的认证数据生成基于风险的认证结果数据，该基于风险的认证结果数据包括用于该交易的风险分数。此外，启用RBA的目录服务器通过将风险分数与监管实体建立的受监管的风险阈值进行比较来确定交易中的欺诈风险低于该受监管的风险阈值。启用RBA的目录服务器还确定交易价值低于监管实体设立的交易限制。交易限制标识阈值交易，对于低于受监管的风险阈值的交易，在低于该阈值交易的情况下可以避免强消费者认证。启用RBA的目录服务器基于所确定的欺诈风险低于受监管的风险阈值并且进一步基于所确定的交易价值低于交易限制来发送认证响应消息，该认证响应消息在没有对交易执行强消费者认证的情况下对交易进行认证。

[0027] 如上所述，在至少一些已知的认证系统中，发行了用于交易的支付卡的银行(称为发行方)与ACS签订合同以用于认证服务。具体地，ACS分析与交易相关联的数据中的至少一些数据、确定声称的持卡人是否可能事实上是实际或合法的持卡人并向发行方报告该确定。在某些市场中，监管者可能会要求对某些类型的交易进行强消费者认证，例如卡不存在(CNP)的交易。此类监管旨在减少在线欺诈，但通常以牺牲客户和商家的满意度为代价。例

如,迫使客户为该市场内100％交易提供密码或密码信息或对文本消息进行响应会增加在线购买环境中的阻力,导致由于客户的沮丧而造成的放弃率增加。

[0028] 因此,为了解决已知认证系统的这些限制,本文描述的系统和方法允许在受监管的市场中更自由地使用SCA的方法。在本文描述的示例实施例中,启用RBA的目录服务器允许低风险、低价值的交易能够避免对消费者的SCA升级质询,同时对高于特定交易价值(例如,高于2000卢比)的交易强制实施SCA,或者对于高于特定风险阈值的交易(例如,“中等”或“高”风险交易)强制实施SCA。

[0029] 更具体地,在示例实施例中,启用RBA的目录服务器允许监管者针对何时可以避免SCA来设定交易价值阈值和风险阈值二者。一些监管者可能会同意,对于某些低风险、低价值的交易,SCA在交易过程中增加的阻力可能不值得在这些情况下欺诈的边际减少。例如,低价值交易中欺诈的发生可能相对较小,并且在这些交易的价值低的情况下,由低价值交易引起的损失量也可能相对较小。此外,如果可以通过基于风险的决策引擎来评估交易风险,那么风险水平低的交易可能只占欺诈的一小部分,从而进一步使其对整体欺诈的贡献边缘化。因此,监管者可以配置启用RBA的目录服务器以在交易价值低并且当交易为欺诈的风险被确定为低时避免SCA。

[0030] 在一些实施例中,启用RBA的目录服务器向监管者提供图形用户界面(GUI),该图形用户界面提供对其受监管的市场内的欺诈的洞察,并且可以允许监管者直接对启用RBA的目录服务器的操作方面进行配置,例如改变用于其市场的条件SCA过程中使用的阈值。GUI可以允许监管者评估现有阈值的当前性能、显示和比较高于或低于所配置的阈值的交易的欺诈数据,例如在特定时段期间欺诈损失的基点。GUI还可以允许监管者评估潜在的阈值,从而基于一组预期阈值提供对欺诈等级的估计。因此,监管者可以使用此类模拟来确定他们如何设定或改变用于他们的市场的阈值。

[0031] 如本文所述,RBA指的是使用通常对发行方或ACS不可用的丰富全面的数据集对交易执行认证。例如,如本文所述,RBA可以包括使用3DS 2协议(例如版本2.0、2.1、2.2和3DS协议的后续版本)执行认证。3DS协议由EMVCo拥有和更新。此外,如本文所述,RBA可以通过由支付处理网络操作的认证平台来执行。因此,出于认证目的,(与由特定ACS处理的相对少量的交易相比)认证平台能够利用先前由支付处理网络处理的所有交易的大量历史交易数据。

[0032] 具体地,在本文描述的系统和方法中,认证系统使用3DS 2协议(或3DS协议的后续版本)进行认证,并且对交易执行RBA以基于监管者配置的阈值价值和风险值确定交易何时可以避免SCA以及何时SCA是强制要求的。启用RBA的目录服务器通信地耦合到RBA引擎(其可以统称为认证平台)。启用RBA的目录服务器和RBA引擎便于评估交易以确定何时强制要求SCA,如本文所述。启用RBA的目录服务器和RBA引擎可以例如由交换网络(例如,支付处理网络)操作。

[0033] 启用RBA的目录服务器从3DS服务器接收认证请求(AReq)消息。启用RBA的目录服务器可以评估交易以(例如,基于商家、商家银行、发行银行、消费者等)确定交易与哪个(哪些)市场相关联。如果交易与如本文所述的配置用于“条件SCA”的受监管的市场相关联,则启用RBA的目录服务器将交易价值与由该相关联的市场的监管者设定的所配置的交易价值阈值进行比较。如果交易价值低于交易价值阈值,则RBA引擎使用交易数据和对启用RBA的

目录服务器可用的其他数据来评估交易的风险。

[0034] 在示例实施例中，由RBA引擎生成的RBA结果数据包括风险分数、风险分析和至少一个原因代码。风险分数是表示所确定的交易风险的分数，较低分数表示较低风险，较高分数表示较高风险。换句话说，风险分数表示可疑持卡人(例如，试图进行交易的人)是具有使用支付卡执行支付交易的特权的合法持卡人的可能性。例如，风险分数可以由0-999的数字和/或0-19的风险阈值类别表示。本领域技术人员将理解，可以使用任何合适的风险分数。

[0035] 风险分析是对应于风险分数的风险等级的描述(例如，低风险、中等风险或高风险)。此外，原因代码包括影响风险分数的一个或多个因素。在一些实施例中，如本文所述，使用原因代码类别和锚来生成原因代码。在一些实施例中，原因代码受规则和/或规则和模型的组合的影响。RBA引擎将RBA结果数据发送到启用RBA的目录服务器。

[0036] 在一些场景中，启用RBA的目录服务器将RBA结果数据嵌入到AReq消息中以生成要被发送到用于该交易的ACS的增强或丰富的AReq消息。例如，在一些实施例中，RBA结果数据作为AReq消息的可扩展标记语言(XML)扩展被追加到AReq消息。例如，该扩展可以具有以下格式：

```
"name": "ACS RBA",
"id": "A000000004-acsRBA",
"criticalityIndicator": "true",
"data": {
```

[0037]

```
"status":"success",
"score":"150",
"decision":"low risk",
"reasonCode1":"Y",
"reasonCode2":"J"}
```

[0038] 其中“score”是风险分数，“decision”是风险分析，“reasonCode1”和“reasonCode2”是原因代码。在示例性实施例中，原因代码每个都作为单个字母发送。在其他实施例中，原因代码可以用不同的方法表示。在一些实施例中，reasonCode2由商家发送以提供商家对交易的评估。替代地，可以使用任何合适的过程将RBA结果数据嵌入到AReq消息中以生成增强或丰富的AReq消息。

[0039] 然后，增强的AReq消息可以从启用RBA的目录服务器发送到ACS。然后，ACS分析增强的AReq消息中的RBA结果数据以做出认证决定。也就是说，在示例实施例中，ACS可以基于风险分数、风险分析和原因代码中的至少一个来确定完全认证交易、拒绝对交易的认证、或者对该交易执行附加认证(例如，通过向持卡人发出升级质询)。因此，ACS可以不执行RBA分析，但仍然能够利用该分析的结果(例如，通过在它们自己的欺诈分析平台中使用这些结

果)来做出认证决定,这通常导致更多的批准并且更少欺诈。因此,启用RBA的目录服务器和RBA引擎可以代表ACS执行RBA分析。在一些实施例中,ACS从多个源接收认证数据。进一步地,启用RBA的目录服务器确定该交易是否如相关联的市场的监管者强制要求的那样需要SCA。

[0040] 在示例实施例中,认证平台将RBA结果数据与存储的认证简档进行比较。该认证简档包含用于处理认证请求的多个规则。在一些实施例中,认证简档由与发行方银行相关联的发行方计算设备提供。规则的示例包括但不限于如何在ACS不可用时继续、要包括在RBA中的信息、发行方提供的风险分数和风险等级的风险等级阈值、决策风险阈值和专门规则(例如所有跨境交易都要提交给ACS)。在一些实施例中,认证简档可以包括监管者施加的针对特定市场的交易阈值价值和针对风险类别的阈值,其定义SCA何时被强制要求。认证简档存储在RBA平台上,并且可以在确定风险分数的任何时候被访问。

[0041] 在示例实施例中,认证平台还将RBA结果数据与认证简档进行比较,以确定与认证请求所关联的交易相关联的风险等级。在一些实施例中,认证平台将风险分数与认证简档中的一个或多个阈值进行比较,以确定与交易相关联的风险等级。在其他实施例中,认证平台将来自RBA结果数据的风险分析、原因代码和/或数据的任何其他组合以及可能的一些或所有认证数据与认证简档进行比较,以确定与此交易相关联的风险等级。例如,风险分数为900或更低可被视为低风险,风险分数在900和980之间可被视为中等风险,风险分数高于980可被视为高风险。本领域技术人员将理解,可以使用任何合适的风险分数阈值和任何数量的风险等级。

[0042] 在示例实施例中,认证平台确定风险等级是否是高风险。在示例实施例中,在高风险交易的情况下,认证平台可以拒绝交易。认证平台可以向3DS服务器发送包括拒绝的认证响应(ARes)消息。3DS服务器可以向商家发送包括拒绝的ARes消息,其中商家确定是否继续授权过程。在这些实施例中,在商家在收到拒绝之后开始授权过程的情况下,该交易被认为是仅商家认证,其中商家承担交易风险。

[0043] 认证平台确定交易是中等风险还是低风险。如果交易是低风险的,则认证平台可批准交易并将包括批准的认证响应(ARes)消息发送到3DS服务器,其中3DS服务器和商家中的至少一个可以发起授权过程。在一些实施例中,如果交易受到受监管的市场的约束,则如果交易低于用于该市场的交易价值阈值,则可以在没有SCA的情况下授权交易,或者,如果交易价值高于用于该市场的阈值,则该交易可以被强制要求受到SCA。如果交易是中等风险,则认证平台可以向持卡人发出升级质询。如果交易受到受监管的市场的约束,那么在该市场中可能强制要求SCA。基于升级质询的结果,认证平台可以批准或拒绝该交易。在一些实施例中,如果交易是中等风险,则认证平台将RBA结果数据发送到ACS,使得ACS将执行该升级质询。在其他实施例中,基于认证简档,认证平台可以在不同的风险等级采用不同步骤,并且具有要分析的附加的或更少的风险等级。

[0044] 3DS 2协议(以及3DS协议的后续版本)为持卡人、发行方和商家提供了许多好处。它通过一种包含丰富全面的数据集以做出认证决定的方法来降低未授权交易的风险。对于持卡人而言,无论支付渠道或设备如何,它都能提供简单、安全且熟悉的在线认证体验。对于发行方而言,它允许“无阻力”认证,其中不需要或不执行显式的持卡人升级认证。这实现了更智能的风险评估决策,并能够根据需要有选择地质询持卡人。这也改善了持卡人的体

验以及对发行方的整体持卡人忠诚度。对于商家而言,3DS 2协议减少了所有经认证的交易的欺诈,并通过减少阻力和减少放弃购物车(即,持卡人在已经选择了要购买的一个或多个商品后决定不完成交易)来增加收入潜力,尤其是对移动支付渠道而言。这也改善了持卡人的体验以及对商家的整体持卡人忠诚度。3DS 2协议和RBA可以支持额外的支付渠道,例如但不限于卡上文件、钱包、移动、应用内和物联网(IoT)。

[0045] 使用3DS 2协议(或3DS协议的后续版本),支付网络可以在其品牌的所有卡上全局查看100%的所有认证请求。包括发行方和ACS提供商在内的任何其他方都无法提供这种全局可见性。可以利用这种全局可见性来代表发行方提供一致的,基于标准的交易风险分析,从而实现全市场的基于风险的认证方法。

[0046] 与先前的认证方法(例如,3DS 1.0)相比,3DS 2协议(以及3DS协议的后续版本)允许收集、分析和利用大约十倍的交易数据量以防止欺诈。3DS协议中包含的附加数据增加了商家和发行方之间的数据交换,并改善了基于风险的认证(RBA)决策。RBA允许发行方通过交易风险分析来检查每个认证请求同时将防欺诈工作集中在防止最大风险的交易上。此外,RBA结合风险引擎利用行为和交易输入二者来确定交易的风险。持卡人认证的RBA方法实时动态计算任何给定电子商务交易的风险评估。该评估然后可以被用来以无阻力的方式对持卡人进行认证。

[0047] RBA方法包括三个部件,它们协同工作以提供对持卡人的认证。首先,底层数据模型用于提供认证的基础。底层数据模型可以包括3DS数据,其可以包括持卡人数据、行为数据、位置数据、商家数据和设备数据。底层数据模型还可以包括交换网络数据,例如但不限于过去的风险分数、认证批准、授权历史、退款数据和欺诈数据。

[0048] RBA方法可以在一种或多种测量方法中用于底层数据模型。这些测量方法可以包括短期速度和比率,包括测量行为一致性和变化,例如频率、花费的金额、时间、位置和设备。测量方法还可以包括长期速度和比率,其包括行为测量和异常检测。测量方法还可以包括跨支付网络的连续测量。

[0049] 然后,RBA方法可以在规则引擎中使用底层数据模型和测量方法。规则引擎可以包括用于解释测量结果的阈值、用于组合测量结果的规则,以及用于将其他数据与模型和测量结合的规则。

[0050] 被认为安全或低风险的交易被静默地认证(即,所谓的“无阻力”认证),而高风险交易受到升级认证。当低风险交易以静默方式进行认证时,已经收集了如此多的数据以至于进一步的认证几乎没有增加任何价值。因此,RBA有效地取代了与持卡人就每笔交易进行显式交互的需要,但交易仍然是完全认证的,责任由发行方承担。因此,更多的交易被完成并且持卡人中断最小,从而帮助电子商务增长。

[0051] 安全(或低风险)交易的示例可以包括,在持卡人具有正面的交易历史的情况下,正在与具有与持卡人的正面关联的已知设备执行交易、持卡人处于典型的地理位置、该设备正在使用典型的IP地址、交易符合典型的行为和交易模式、并且配送地址已与支付帐号(PAN)一起使用过并且与上次交易相同。持卡人购买礼物送到他家。中等风险交易的示例可以包括,在持卡人具有正面的交易历史的情况下,使用与持卡人没有已知关联的未知设备,该设备处于非典型的地理位置和IP地址,但是是典型的行为、持卡人和交易模式。例如,持卡人正在旅行并在酒店购买互联网接入。高风险交易的示例可以包括,在网络中的持卡人

检测到异常速度的情况下，使用与持卡人没有已知关联的未知设备，该设备处于非典型的地理位置和IP地址，并且检测到异常行为模式。在持卡人在圣路易斯购买午餐后，持卡人在德克萨斯购买了超过600美元的服装。

[0052] RBA的一个目标是最小化需要主动(即，升级)认证的交易的数量，同时将欺诈保持在最低限度并且在交易过程期间改善消费者阻力点。RBA的目标是静默地消除低风险交易的不必要阻力。大约90％的交易被视为低风险，然后在没有任何动作的情况下通过认证，并将进入授权流程。这大大减少了认证交易所需的处理量和消息流量。5-8％的交易将被视为中等风险，并且将例如通过升级质询来要求持卡人自我认证。然后1-2％的交易将被视为高风险并且将不通过认证。利用RBA，所收集的信息使得交易能够被评分和分类成为低、中、高风险，允从而许发行方和ACS采取适当的动作。

[0053] 3DS 2协议(以及3DS协议的后续版本)实现对到达目录服务器510的所有交易的全市场应用风险分析。可以使用3DS 2协议(以及3DS协议的后续版本)基于可用的全局数据对每个交易进行评分和/或标记。另外，操作目录服务器510的支付处理者具有跨数字域和物理域查看持卡人活动的能力，并且可以利用该扩展视图来改进评分。相反，传统的认证服务提供商可能只处理数字域。例如，支付处理者可以指示特定设备是否与欺诈相关联，并且在将来的交易中为发行方标记该设备。然后，发行方可以拒绝涉及该设备的交易或提示进行附加认证(例如，通过双因素认证)。

[0054] 下面的表1列出了3DS 2协议中用于认证的许多数据元素。例如，这些数据元素中的至少一些可以被包括在发送到目录服务器510的AReq中所包括的认证数据中。也是3DS 1.0协议的一部分的十八个数据元素在表1中以粗体表示。本领域技术人员将理解的是，丰富数据元素的数量(例如，在3DS协议的未来版本中)可以增长到超出下面列出的数量，并且可以包括超过一百七十个数据元素。此外，基于应用的(例如，使用移动计算设备执行)交易可以提供比基于浏览器的交易更多的数据元素。此外，使用Android设备执行的交易可能有超过一百三十个附加元素。认证数据还可以按类别划分，例如：交易数据(金额、货币、日期和时间)、设备数据(IP地址、设备信息和渠道数据)、持卡人数据(帐号和配送地址)和商家数据(名称、类别和国家)。

[0055]

	数据元素
1	3DS 请求者认证信息
2	3DS 请求者质询指示符
3	3DS 请求者 ID
4	3DS 请求者发起的指示符
5	3DS 请求者名称
6	3DS 请求者非支付认证指示符
7	3DS 请求者先前交易认证信息
8	3DS 请求者 URL

[0056]

	数据元素
9	3DS 服务器运营商 ID
10	3DS 服务器参考编号
11	3DS 服务器交易 ID
12	3DS 服务器 URL
13	帐户类型
14	**收单方 BIN**
15	**收单方商家 ID**
16	ACS 质询强制指示符
17	ACS 计数器 ACS 到 SDK
18	**ACS HTML**
19	ACS 运营商 ID
20	ACS 参考编号
21	ACS 呈现类型
22	**ACS 签名内容**
23	ACS 交易 ID
24	ACS UI 类型
25	地址匹配指示器
26	认证方法
27	验证类型
28	**认证值**
29	浏览器接受头部
30	浏览器 IP 地址
31	浏览器 Java 已启用
32	浏览器语言
33	浏览器屏幕色深
34	浏览器屏幕高度
35	浏览器屏幕宽度
36	浏览器时区
37	浏览器用户代理
38	卡/令牌有效期
39	持卡人帐户标识符
40	持卡人账户信息
41	**持卡人账号**
42	持卡人账单地址城市
43	持卡人账单地址国家
44	持卡人账单地址 行 1
45	持卡人账单地址 行 2
46	持卡人账单地址 行 3
47	持卡人账单地址邮政编码
48	持卡人账单地址状态
49	持卡人电子邮件地址
50	持卡人家庭电话号码

[0057]

	数据元素
51	持卡人移动电话号码
52	持卡人姓名
53	持卡人配送地址城市
54	持卡人配送地址国家
55	持卡人配送地址 行 1
56	持卡人配送地址 行 2
57	持卡人配送地址 行 3
58	持卡人配送地址邮政编码
59	持卡人配送地址状态
60	持卡人工作电话号码
61	质询附加信息文本
62	质询取消指示符
63	质询数据入口
64	质询 HTML 数据入口
65	质询信息标题
66	质询信息标签
67	质询信息文本
68	质询信息文本指示符
69	质询选择信息
70	质询窗口大小
71	设备信道
72	设备信息
73	支持的设备呈现选项
74	DS 参考编号
75	DS 交易 ID
76	DSURL
77	电子商务指示符
78	EMV 支付令牌指示符
79	可扩展信息标签 1
80	可扩展信息文本 1
81	分期付款数据
82	交互柜台
83	发行方图像
84	商家类别代码
85	**商家国家代码**
86	**商家名称**
87	商家风险指示符
88	消息类别
89	**消息扩展**
90	**消息类型**
91	**消息版本号**
92	通知 URL

[0058]

	数据元素
93	OOB 应用标签
94	OOB 应用 URL
95	OOB 继续指示符
96	OOB 继续标签
97	支付系统图像
98	**购买量**
99	**购买货币**
100	**购买货币指数**
101	**购买日期和时间**
102	**循环的到期**
103	**循环频率**
104	重新发送质询信息代码
105	重新发送信息标签
106	结果消息状态
107	SDK 应用 ID
108	SDK 计数器 SDK 到 ACS
109	SDK 加密数据
110	SDK 临时公钥（Qc）
111	SDK 参考编号
112	SDK 交易 ID
113	提交认证标签
114	**交易状态**
115	交易状态原因
116	交易类型
117	原因信息标签
118	原因信息文本

[0059] 表1

[0060] 在示例实施例中，交易被分类为“仅商家(merchant-only)”或“完全认证(fully authenticated)”。“完全认证”交易通常被认为是已经认证的低风险交易。“仅商家”交易是风险更大的交易。在一些实施例中，“仅商家”交易已被认证。在示例实施例中，认证响应中的一个或多个指示符指示交易是“仅商家”还是“完全认证”。一个或多个指示符还可以指示是否对交易上尝试了认证。商家使用该信息来确定是否开始针对交易的授权过程。在一些实施例中，该信息也存储在数据库中，并且在授权过程期间由交换网络和发行方处理者中的至少一个引用。

[0061] 在一些另外的实施例中，认证平台确定认证请求消息是否符合3DS 2协议或3DS协议的后续版本。如果认证请求消息不符合适当的3DS协议，则认证平台绕过确定ACS是否可用。在这种情况下，认证平台发送认证响应消息，该消息指示该交易仅被视为仅商家的并且未尝试认证。

[0062] 在一些实施例中，认证平台基于RBA结果数据确定风险等级。如果风险等级为低，则认证平台在认证响应消息中嵌入指示符，从而指示该交易是“完全认证的”。如果风险等级不为低，则认证平台在认证响应消息中嵌入一个或多个指示符，从而指示该交易是仅商

家的交易并且尝试了认证。

[0063] 在示例实施例中，认证平台对交易执行认证过程，包括RBA。该分析基于机器学习模型，随着时间的推移，认证平台能够提高其确定与交易相关的风险等级的能力。认证平台分析由ACS认证的交易，并将这些交易与历史数据进行比较，以为每个发行方生成风险模型。通过比较每个交易中的数据点，风险模型将基于相应的认证请求中的认证数据指示与每个交易相关联的风险量。这允许认证平台在ACS不可用时对交易进行分析，并对这些交易执行认证以提供对认证请求的响应。因此，认证平台可以确定所接收的授权请求与ACS评分为低风险的先前交易基本上类似。因此，允许认证平台以一定程度的确定性确定所接收的交易是低风险的。

[0064] 该系统解决的至少一个技术问题包括：(i)高网络负荷，其至少部分地基于对大多数或所有的卡不存在的交易的升级质询，这导致网络延迟和减少的带宽；(ii)如果没有对卡不存在的交易的升级质询，则允许欺诈交易被成功处理；(iii)至少部分地基于在交易期间必须应答附加的认证质询而在卡不存在的交易期间的消费者不便；(iv)消费者在面临升级质询时放弃交易，从而导致商家的销售损失以及基于这些被放弃的交易的其他网络方的处理费损失；(v)无法向商家和/或商家收单方提供可定制的欺诈相关服务；(vi)商家对欺诈交易的责任风险增加；(vii)与数字钱包有关的欺诈；(viii)发行方对某些可能用于欺诈评分交易的数据的访问权限有限；(ix)通过减少进出ACS的网络流量来减少网络负荷；(x)通过减少所需的步骤数来提高认证过程的速度；(xi)通过预过滤认证请求来减少ACS的处理负荷，以防止冗余或不必要的处理；以及(xii)提高的交易批准率。

[0065] 通过执行以下步骤中的至少一个来实现本文描述的系统和过程的技术效果：(i)接收用于交易的认证请求消息，该认证请求消息包括认证数据；(ii)从认证请求消息中提取认证数据；(iii)确定ACS是否可用于处理该交易；(iv)如果ACS不可用，则至少一个处理器被编程为：(a)至少部分地基于所提取的认证数据生成包括风险分数和至少一个原因代码的基于风险的认证(RBA)结果数据，该至少一个原因代码指示影响了所生成的风险分数的至少一个因素；(b)将认证数据与至少一个长期变量和至少一个短期变量进行比较，其中至少一个长期变量包括历史认证数据和历史授权数据；(c)基于RBA结果数据发送认证响应消息；(v)基于提取的认证数据确定在线用户不与ACS相关联；(vi)基于RBA结果数据生成认证决定；(vii)基于RBA结果数据确定风险等级；(viii)如果风险等级低，则在认证响应消息中嵌入指示符，该指示符指示交易被完全认证；(ix)如果风险等级不为低，则在认证响应消息中嵌入一个或多个指示符，该一个或多个指示符指示该交易是仅商家交易并且尝试了认证；(x)确定认证请求消息是否符合3DS 2协议或3DS协议的后续版本；(xi)如果认证请求消息不符合，则绕过确定ACS是否可用。

[0066] 在一些实施例中，通过执行以下步骤中的至少一个来实现进一步的技术效果：(i)将认证请求消息发送到ACS；(ii)等待来自ACS的响应达到预定时间段；(iii)如果在预定时间段之后没有收到响应，则确定ACS不可用；(iv)从ACS接收响应，其中该响应指示在线用户中的至少一个未向ACS注册、ACS当前不可用，并且ACS无法认证该在线用户。

[0067] 在一些实施例中，通过执行以下步骤中的至少一个来实现附加的技术效果：(i)接收涉及由监管实体监管的市场的交易的认证请求消息，该认证请求消息包括认证数据和交易价值；(ii)从认证请求消息中提取认证数据；(iii)至少部分地基于所提取的认证数据生

成基于风险的认证(RBA)结果数据,该基于风险的认证(RBA)结果数据包括交易的风险分数;(iv)通过将风险分数与监管实体建立的受监管的风险阈值进行比较,确定交易中的欺诈风险低于该受监管的风险阈值;(v)确定交易价值低于监管实体设定的交易限制,该交易限制标识阈值交易,对低于受监管的风险阈值的交易,在低于该阈值交易的情况下可以避免强消费者认证;(vi)基于所确定的欺诈风险低于受监管的风险阈值并且进一步基于所确定的交易价值低于交易限制来发送认证交易的认证响应消息,而不对交易执行强消费者认证。

[0068] 基于本文的描述,将理解的是,如本文所述的认证系统中的技术改进是针对本身植根于计算机技术(例如,问题本身源于使用计算机技术)的技术缺陷或问题的基于计算机的解决方案。更具体地,欺诈是通过电子支付网络进行的交易的重要问题,尤其是对于卡不存在的交易。存在高级欺诈检测方法(例如,RBA),但是至少一些ACS不能执行那些方法,并且此外与ACS的通信增加了网络流量和处理负荷,并且此外ACS可能会不可用。因此,为了解决该问题,本文描述的系统和方法通过使用启用RBA的目录服务器和RBA引擎执行RBA并对结果进行过滤以确定哪些认证需要被转发到ACS以及将RBA的结果转发到ACS以使ACS能够做出认证决定,从而解决该技术问题。

[0069] 以下对本公开的实施例的详细描述参考附图。不同附图中的相同附图标记可标识相同或相似的元件。而且,以下详细描述不限制权利要求。

[0070] 本文描述的是诸如认证计算机系统的计算机系统。如本文所述,所有这样的计算机系统包括处理器和存储器。然而,本文提到的计算机设备中的任何处理器也可以指代一个或多个处理器,其中处理器可以在一个计算设备中或多个并行工作的计算设备中。另外,本文提到的计算机设备中的任何存储器还可以指一个或多个存储器,其中存储器可以在一个计算设备中或多个并行工作的计算设备中。

[0071] 如本文所使用的,处理器可以包括任何可编程系统,包括使用微控制器、精简指令集电路(RISC)、专用集成电路(ASIC)、逻辑电路以及能够执行本文所述功能的任何其他电路或处理器的系统。以上示例仅是示例,因此不旨在以任何方式限制术语“处理器”的定义和/或含义。

[0072] 如本文所使用的,术语“数据库”可以指数据主体、关系数据库管理系统(RDBMS)或两者。如本文所使用的,数据库可以包括任何数据集合,包括分层数据库、关系数据库、平面文件数据库、对象关系数据库、面向对象的数据库,以及存储在计算机系统中的任何其他结构化的记录或数据集合。以上示例仅是示例,因此不旨在以任何方式限制术语数据库的定义和/或含义。RDBMS的示例包括但不限于包括**Oracle®**数据库、MySQL、**IBM®**DB2,**Microsoft®** SQLServer,**Sybase®**和PostgreSQL。然而,可以使用任何能够实现本文描述的系统和方法的数据库。(Oracle是Oracle Corporation,Redwood Shores,California的注册商标;IBM是International Business Machines Corporation,Armonk,New York的注册商标;Microsoft是Microsoft Corporation,Redmond,Washington的注册商标;Sybase是Sybase,Dublin,California的注册商标。)

[0073] 在一个实施例中,提供了一种计算机程序,并且该程序被实施在计算机可读介质上。在示例实施例中,系统在单个计算机系统上执行,而不需要连接到服务器计算机。在还

有的示例实施例中，系统在Windows®环境(Windows是Redmond，Washington的Microsoft公司的注册商标)中运行。在又一个实施例中，系统在大型机环境和UNIX®服务器环境(UNIX是位于Reading，Berkshire，United Kingdom的X/Open有限公司的注册商标)上运行。在另一个实施例中，系统在iOS®环境(iOS是位于San Jose，CA的Cisco系统公司的注册商标)上运行。在又一个实施例中，系统在Mac OS®环境(Mac OS是位于Cupertino，CA的Apple公司的注册商标)上运行。在又一个实施例中，系统在Android®环境(Android是Mountain View，CA的Google公司的注册商标)上运行。在又一个实施例中，系统在Linux®环境(Linux是Boston，MA的Linux Torvalds的注册商标)上运行。应用是灵活的并且被设计为在各种不同环境中运行，而不会损害任何主要功能。在一些实施例中，系统包括分布在多个计算设备中的多个组件。一个或多个组件是实施在计算机可读介质中的计算机可执行指令的形式。

[0074] 如本文所使用的，以单数形式叙述并且以单词“一”或“一个”开头的元件或步骤应该被理解为不排除多个元件或步骤，除非明确地叙述了这种排除。另外，对本公开的“实例实施例”或“一个实施例”的引用不旨在被解释为排除也包含所述特征的另外的实施例的存在。

[0075] 如本文所使用的，术语“软件”和“固件”是可互换的，并且包括存储在存储器中以供处理器执行的任何计算机程序，包括RAM存储器、ROM存储器、EPROM存储器、EEPROM存储器和非易失性RAM(NVRAM)存储器。上述存储器类型仅仅是示例，并且因此对于可用于存储计算机程序的存储器的类型没有限制。

[0076] 如本文所使用的，术语“支付设备”、“交易卡”、“金融交易卡”和“支付卡”是指任何合适的交易卡，诸如信用卡、借记卡、预付卡、收费卡、会员卡、促销卡、常旅客卡、身份证、预付卡、礼品卡，和/或可以持有支付账户信息的任何其它设备，诸如移动电话、智能电话、个人数字助理(PDA)、可穿戴计算设备、密钥卡和/或能够提供账户信息的任何计算设备。此外，这些术语可以指从银行账户、存储的数值账户、移动钱包等直接进行的支付或使用其进行的支付，并且相应地不限于物理设备，而是一般地指支付凭据。每种类型的交易设备都可以用作执行交易的支付方法。此外，消费者卡账户行为可以包括但不限于购买、管理活动(例如，余额检查)、账单支付、目标的实现(满足账户余额目标、按时支付账单)和/或产品注册(例如，移动应用下载)。

[0077] 系统和处理不限于本文描述的具体实施例。此外，每个系统的组件和每个处理可以与本文描述的其它组件和处理分开地和独立地实践。每个组件和处理也可以与其它组装包和处理结合使用。

[0078] 以下详细描述通过示例而非限制的方式示出了本公开的实施例。预期本公开具有认证用户以通过电子支付网络进行交易的一般应用。

[0079] 图1是图示根据本公开的一个示例性实施例的示例性RBA平台34的示意图，其与多方支付卡系统20通信以处理支付交易。图1描绘了金融交易通道系统20中的数据流。本文描述的实施例可涉及支付卡系统，诸如使用MasterCard®交换网络的信用卡支付系统。MasterCard®交换网络是由MasterCard国际公司®颁布的一组专有通信标准，用于

在作为MasterCard国际公司®的成员的金融机构之间交换金融交易数据和结算资金(MASTERCARD®是位于Purchase,New York的MasterCard国际公司的注册商标)。

[0080] 在示例性交易卡系统中,称为“发行方”的金融机构发行支付卡(诸如信用卡)给消费者或持卡人22,消费者或持卡人22使用交易卡为从商家24的购买进行付款。持卡人22可以在商家24处购买商品或服务(“产品”)。持卡人22可以使用虚拟形式的交易卡来进行这种购买,更具体地,可以通过提供与交易卡相关的数据(例如,交易卡号码、有效日期、相关联的邮政编码以及安全码)来发起交易。为了接受用交易卡或虚拟形式的交易卡支付,商家24通常必须与作为金融支付系统的一部分的金融机构建立账户。该金融机构通常被称为“商家银行”或“收单银行”或“收单方”。在示例实施例中,当持卡人22用交易卡或虚拟交易卡对购买进行付款时,商家24针对购买金额从商家银行26请求对持卡人22的认证和授权。该请求可以通过电话执行或电子地执行,但通常通过使用销售点终端来执行,销售点终端27从交易卡上的磁条、芯片、浮雕字符等读取持卡人22的账户信息,并与商家银行26的交易处理计算机电子地通信。商家24接收由持卡人22提供的持卡人22的账户信息。替代地,商家银行26可以授权第三方代表其执行交易处理。在这种情况下,销售点终端将被配置为与第三方通信。这样的第三方通常被称为“商家处理者”、“收单处理者”或“第三方处理者”。

[0081] 使用交换网络28,商家处理者或商家银行26的计算机将与发行方银行30的计算机通信,以确定指称持卡人是否实际为合法持卡人22(即,认证),持卡人22的账户32是否信誉良好,以及持卡人的可用信用额度是否涵盖购买。基于这些确定,认证和授权请求将被拒绝或接受。可以在授权之前执行认证。如果请求被接受,则授权码被发布给商家24。

[0082] 在示例性实施例中,支付卡系统20包括基于风险的认证(RBA)平台34或与之通信。在该实施例中,RBA平台34提供增强的元数据收集以捕获信息,包括来自由支付卡系统20处理的支付交易的元数据。RBA平台34存储该元数据,以在执行授权处理之前执行认证处理时提供其作为历史数据。在示例性实施例中,RBA平台34可以从收单方银行26、交换网络28和发行方银行30中的一个或多个接收历史数据。该数据的示例包括一个或多个长期变量(“LTV”)。一个或多个LTV可以包括与多个PAN相关联的历史授权数据、与多个PAN相关联的其他历史数据等。LTV可以与卡存在和卡不存在的历史交易二者相关联。例如,LTV可以包括持卡人配送地址、持卡人账单地址、持卡人电子邮件地址、持卡人电话号码、商家名称、商家类别、商家位置和/或至少一个与环境相关的变量(例如,设备细节、浏览器细节),包括设备ID、IP地址、设备信道等。此外,LTV可以存储在RBA平台34可访问的数据库中并由交换网络28操作。在一些实施例中,LTV数据将在存储之前被散列化以保护此个人身份信息的安全性。

[0083] 当授权请求被接受时,持卡人22的账户32的可用信用额度减少。通常,支付卡交易的费用没有立即过账到持卡人22的账户32,因为银行卡协会(诸如Mastercard国际公司®)已颁布直到货物被运送或服务被交付才允许商家24对交易收费或“捕获”的规则。但是,对于至少一些借记卡交易,费用可以在交易时过账。当商家24运送或交付货物或服务时,商家24通过例如在销售点终端上的适当的数据输入过程来捕获交易。这可以包括对标准零售购买每日集束已批准的交易。如果持卡人22在交易被捕获之前取消交易,那么生成“无效(void)”。如果持卡人22在交易已被捕获之后退货,那么生成“信用”。交换网络

28和/或发行方银行30在数据库120(在图2中示出)中存储交易卡信息,诸如购买类型、购买金额、购买日期。

[0084] 在进行购买之后,发生清算过程以在交易各方(例如商家银行26、交换网络28和发行方银行30)之间转移与购买有关的附加交易数据。更具体地,在清算过程期间和/或在清算过程之后,与交易相关联的附加数据(例如购买时间、商家名称、商家类型、购买信息、持卡人帐户信息、交易类型、关于所购买的商品和/或服务的信息、和/或或者其他合适的信息)作为交易数据在交易各方之间传输,并且可以由交易的任何一方存储。在交易被授权和清算之后,交易在商家24、商家银行26和发行方银行30之间结算。结算是指与交易相关的商家24的账户、商家银行26和发行方银行30之间的金融数据或资金的转移。通常,交易被捕获并累积成"批",该"批"作为组结算。更具体地,交易可以在发行方银行30和交换网络28之间结算,然后在交换网络28和商家银行26之间结算,然后在商家银行26和商家24之间结算。

[0085] 如下面更详细地描述的,在多方支付卡系统20的背景下,可以由RBA平台34代表接入控制服务器(ACS)或发行方银行30来执行基于风险的认证(RBA)。尽管这里描述的系统不旨在限于促进这样的应用,但是出于示例目的,系统被描述为这样的。

[0086] 图2是用于认证支付交易的计算机系统100的示例实施例的扩展框图。在示例性实施例中,系统100可用于与ACS一致地或代替ACS来验证支付交易。

[0087] 在示例性实施例中,持卡人计算设备102是包括网络浏览器或软件应用的计算机,其使得持卡人计算设备102能够使用互联网或其他网络访问诸如商家网站104之类的远程计算机设备。更具体地,持卡人计算设备102可以通过许多接口通信地耦合到互联网,所述接口包括但不限于至少一种网络,诸如互联网、局域网(LAN)、广域网(WAN)或综合业务数字网(ISDN)、拨号连接、数字用户线路(DSL),蜂窝电话连接和线缆调制解调器。持卡人计算设备102可以是能够访问互联网的任何设备,包括但不限于台式计算机、膝上型计算机、个人数字助理(PDA)、蜂窝电话、智能电话、平板电脑、平板手机、可穿戴电子设备、智能手表或其他基于网络的可连接设备或移动设备。在示例性实施例中,持卡人计算设备102与各个持卡人22(图1中所示)相关联。

[0088] 在示例性实施例中,商家网站104是可通过计算机访问的在线购物网站,该计算机包括使用互联网或其他网络的网络浏览器或软件应用,例如持卡人计算设备102。更具体地,商家网站104可以托管在通过许多接口通信地耦合到互联网的一个或多个计算机上,所述接口包括但不限于至少一种网络,诸如互联网、局域网(LAN)、广域网(WAN)或综合业务数字网(ISDN)、拨号连接、数字用户线路(DSL),蜂窝电话连接和线缆调制解调器。计算设备托管的商家网站104可以是能够访问互联网的任何设备,包括但不限于台式计算机、膝上型计算机、个人数字助理(PDA)、蜂窝电话、智能电话、平板电脑、平板手机、可穿戴电子设备、智能手表或其他基于网络的可连接设备或移动设备。在示例性实施例中,商家网站104与商家24(图1中所示)相关联。在示例性实施例中,商家网站104允许持卡人22使用持卡人计算设备102购买商品和/或服务。在一些实施例中,通过商家网站104执行的支付交易被认为是卡不存在的交易。

[0089] 在示例性实施例中,数据收集计算机设备106是包括网络浏览器或软件应用的计算机,其使得数据收集计算机设备106能够使用互联网或其他网络访问远程计算机设备,例如商家网站104和认证服务器112。更具体地,数据收集计算设备106可以通过许多接口通信

地耦合到互联网，所述接口包括但不限于至少一种网络，诸如互联网、局域网(LAN)、广域网(WAN)或综合业务数字网(ISDN)、拨号连接、数字用户线路(DSL)，蜂窝电话连接和线缆调制解调器。数据收集计算设备106可以是能够访问互联网的任何设备，包括但不限于台式计算机、膝上型计算机、个人数字助理(PDA)、蜂窝电话、智能电话、平板电脑、平板手机、可穿戴电子设备、智能手表或其他基于网络的可连接设备或移动设备。在一些实施例中，数据收集计算机设备106与3DS服务器或服务相关联。在其他实施例中，数据收集计算机设备106与收单方银行26(如图1所示)相关联。

[0090] 在示例性实施例中，认证服务器112与多个数据收集计算机设备106和一个或多个接入控制服务器(ACS)108通信。在一些实施例中，认证服务器112类似于RBA平台34(在图1中示出)。在示例性实施例中，认证服务器112从数据收集计算机设备106接收数据并使用该数据来执行支付交易的认证。在一些实施例中，认证服务器112执行与ACS 108的认证。在其他实施例中，认证服务器112在认证过程中替换ACS 108。在示例性实施例中，认证服务器112与交换网络28(图1中示出)相关联。在其他实施例中，认证服务器112仅与交换网络28通信。

[0091] 在示例性实施例中，发行方计算设备110是包括网络浏览器或软件应用的计算机，其使得发行方计算设备110能够使用互联网或其他网络访问远程计算机设备，例如ACS 108和认证服务器112。更具体地，发行方计算设备110可以通过许多接口通信地耦合到互联网，所述接口包括但不限于至少一种网络，诸如互联网、局域网(LAN)、广域网(WAN)或综合业务数字网(ISDN)、拨号连接、数字用户线路(DSL)，蜂窝电话连接和线缆调制解调器。发行方计算设备110可以是能够访问互联网的任何设备，包括但不限于台式计算机、膝上型计算机、个人数字助理(PDA)、蜂窝电话、智能电话、平板电脑、平板手机、可穿戴电子设备、智能手表或其他基于网络的可连接设备或移动设备。在示例性实施例中，发行方计算设备110与发行方银行30(如图1所示)相关联。

[0092] 数据库服务器116连接到数据库120。在一个实施例中，集中式数据库120存储在服务器系统112上，并且可以由潜在用户在一个客户端系统(未示出)处通过经由一个客户端系统登录认证服务器112来访问。在替代实施例中，数据库120远离认证服务器112存储，并且可以是非集中式的。数据库120可以是被配置为存储由认证服务器112使用的信息的数据库，所述信息包括例如历史支付交易记录。

[0093] 数据库120可以包括具有分开的区段或部分的单个数据库，或者可以包括多个数据库，其中每个数据库彼此分开。数据库120可以存储在处理网络上生成的交易数据，包括与商家、消费者、账户持有者、预期消费者、发行方、收单方和/或所进行的购买相关的数据。数据库120还可以存储账户数据，包括持卡人姓名、持卡人地址、账号、其他账户标识符和交易信息中的至少一个。数据库120还可以存储商家信息，包括标识注册为使用网络的每个商家的商家标识符，以及用于结算交易的指令(包括商家银行账户信息)。数据库120还可以存储与持卡人从商家购买的物品相关联的购买数据，以及认证和授权请求数据。数据库120可以存储一个或多个认证简档，其中每个认证简档包括一个或多个认证规则，一个或多个风险等级阈值，以及基于风险等级阈值的一个或多个路由规则。

[0094] 图3示出了根据本公开的一个示例实施例的诸如RBA平台34(图1中示出)的服务器系统301的示例配置。服务器系统301还可以包括但不限于商家网站104、数据收集计算机设

备106、ACS 108、发行方计算设备110、认证服务器112和数据库服务器116(均在图2中示出)。在示例实施例中,服务器系统301确定并分析在支付交易中使用的设备的特征,如下所述。

[0095] 服务器系统301包括用于执行指令的处理器305。例如,指令可以存储在存储器区域310中。处理器305可以包括用于执行指令的一个或多个处理单元(例如,在多核配置中)。指令可以在服务器系统301上的各种不同操作系统内执行,诸如UNIX、LINUX、Microsoft Windows®等。还应该认识到的是,一经发起基于计算机的方法,就可以在初始化期间执行各种指令。可能需要一些操作以便执行本文描述的一个或多个处理,而其它操作可能更通用和/或特定于特定编程语言(例如,C、C#、C++、Java或其它合适的编程语言)。

[0096] 处理器305可操作地耦合到通信接口315,使得服务器系统301能够与诸如用户系统或另一个服务器系统301之类的远程设备通信。例如,通信接口315可以经由互联网从客户端系统(未示出)接收请求,如图2所示。

[0097] 处理器305还可以可操作地耦合到存储设备334。存储设备334是适用于存储和/或检索数据的任何计算机操作的硬件。在一些实施例中,存储设备334集成在服务器系统301中。例如,服务器系统301可以包括一个或多个硬盘驱动器作为存储设备334。在其它实施例中,存储设备334在服务器系统301外部,并且可以由多个服务器系统301访问。例如,存储设备334可以包括多个存储单元,诸如在廉价盘冗余阵列(RAID)配置中的硬盘或固态盘。存储设备334可以包括存储区域网络(SAN)和/或网络附接存储(NAS)系统。

[0098] 在一些实施例中,处理器305经由存储接口320可操作地耦合到存储设备334。存储接口320是能够向处理器305提供对存储设备334的访问的任何组件。存储接口320可以包括例如高级技术附件(ATA)适配器、串行ATA(SATA)适配器、小型计算机系统接口(SCSI)适配器、RAID控制器、SAN适配器、网络适配器和/或向处理器305提供对存储设备334的访问的任何组件。

[0099] 存储器区域310可以包括但不限于诸如动态RAM(DRAM)或静态RAM(SRAM)之类的随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)和非易失性RAM(NVRAM)。上述存储器类型仅仅是示例性的,并且因此对于可用于存储计算机程序的存储器的类型没有限制。

[0100] 图4示出了客户端计算设备402的示例配置。客户端计算设备402可以包括但不限于持卡人计算设备102(图1中示出)。客户端计算设备402包括用于执行指令的处理器404。在一些实施例中,可执行指令存储在存储区域406中。处理器404可包括一个或多个处理单元(例如,在多核配置中)。存储区域406是允许存储和检索诸如可执行指令和/或其他数据的信息的任何设备。存储区域406可以包括一个或多个计算机可读介质。

[0101] 客户端计算设备402还包括用于向用户400呈现信息的至少一个媒体输出组件408。媒体输出组件408是能够向用户400传送信息的任何组件。在一些实施例中,媒体输出组件408包括输出适配器,诸如视频适配器和/或音频适配器。输出适配器可操作地耦合到处理器404并且可操作地耦合到输出设备,诸如显示设备(例如,液晶显示器(LCD)、有机发光二极管(OLED)显示器、阴极射线管(CRT)或“电子墨水”显示器)或音频输出设备(例如,扬声器或耳机)。

[0102] 在一些实施例中,客户端计算设备402包括用于从用户400接收输入的输入设备

410。输入设备410可以包括例如键盘、指点设备、鼠标、手写笔(stylus)、触敏面板(例如,触摸板或触摸屏)、相机、陀螺仪、加速度计、位置检测器和/或音频输入设备。诸如触摸屏的单个组件可以既用作媒体输出组件408的输出设备又用作输入设备410。

[0103] 客户端计算设备402还可以包括通信接口412,其可通信地耦合到诸如服务器系统301或由商家操作的网络服务器的远程设备。通信接口412可以包括例如用于与移动电话网络(例如,全球移动通信系统(GSM)、3G、4G或蓝牙)或其它移动数据网络(例如,全球微波接入互操作性(WIMAX))一起使用的有线或无线网络适配器或无线数据收发器。

[0104] 图5是示出使用3DS 2协议(或3DS协议的后续版本)进行认证的示例认证系统500中的交易流的示意图。有关3DS协议的信息,包括协议的当前版本,可见于https://www.emvco.com。系统500包括目录服务器510,其有助于验证持卡人以进行交易,如本文所述。目录服务器510可以例如通过交换网络28(如图1所示)来操作。

[0105] 持卡人(例如,图1中所示的持卡人22)在持卡人计算设备102(图2中示出,例如移动计算设备)上发起交易(例如,在线交易)。在发起交易期间,持卡人提供最终将用于认证持卡人的认证数据。在示例性实施例中,该认证数据包括持卡人填写以进行购买的表格数据以及获取的数据,所述获取的数据是关于持卡人的数据,例如设备细节和包括设备ID、IP地址、设备信道等的浏览器细节。

[0106] 认证数据从持卡人计算设备102发送到3DS请求者环境504内的3DS客户端502。3DS客户端502可以由商家(例如,商家24,如图1所示)操作。在一些实施例中,3DS客户端502是商家网站104的一部分(如图2所示)。3DS客户端502从持卡人计算设备102收集使用3DS 2协议认证持卡人所需的信息,包括认证数据。

[0107] 3DS客户端502收集信息(包括认证数据)并将收集的信息发送到3DS服务器506以包括在认证请求消息中,在此也称为AReq消息。3DS客户端502也是3DS请求者环境504的一部分。3D客户端502和3DS服务器506可以彼此通信,例如,使用应用编程接口(API)或浏览器交互。在一些实施例中,3DS服务器506类似于数据收集计算机设备106(图2中所示)。

[0108] 使用由持卡人提供的认证数据和在3DS请求者环境504内收集的其他数据,3DS服务器506基于与交易中使用的交易卡相关联的支付处理器生成AReq消息并将AReq消息发送到目录服务器510。在一些实施例中,目录服务器510类似于认证服务器112(图2中所示)。也就是说,不同的支付处理器通常将具有用于处理交易的不同目录服务器。当生成AReq消息时,3DS服务器506为了安全目的而格式化数据。在该实施例中,目录服务器510基于支付卡的发行方将AReq消息转发到适当的接入控制服务器(ACS)512。在一些实施例中,ACS 512类似于ACS 108(图2中所示)。

[0109] ACS 512基于AReq消息确定是否需要认证。此外,ACS 512有助于确保适当地执行任何所需的认证。ACS 512代表操作发行方计算设备514的发行方执行这些认证操作。

[0110] 响应于AReq消息,ACS 512向目录服务器510返回认证响应(ARes)消息,目录服务器510进而将其转发到3DS服务器506。在返回ARes消息之前,ACS 512评估AReq消息中的数据,并且对交易执行基于风险的认证(RBA)。具体地,当ACS 512确定不需要显式持卡人升级认证时(即,当确定交易为低风险时),ACS 512确定认证完成并返回指示认证完成的ARes。然而,如果ACS 512确定需要持卡人升级认证,则ACS 512发起升级质询请求。将升级质询请求的结果(在ARes消息中)发送到3DS服务器506(经由目录服务器510),并最终发送给持卡

人。如果需要升级认证，则ACS 512根据用于发行方的持卡人的方法(例如，生物认证、一次性密码(OTP)认证、短消息服务(SMS)认证等)来控制升级认证。包括在3DS请求者环境504中的3DS请求者516控制各种组件在示例实施例中如何彼此交互。

[0111] 在认证过程完成之后(即，在3DS协议结束之后)，如果持卡人被成功认证，则进行交易的支付授权。也就是说，使用3DS 2协议(或3DS协议的后续版本)的认证发生在交易的支付授权之前。

[0112] 对于支付授权，商家(例如，使用3DS服务器506)与由收单方(例如商家银行26(图1中所示))和支付网络522(例如交换网络28(如图1所示))操作的收单方计算设备520交换授权数据。如果合适，则商家、收单方或支付网络可以提交包括指示认证已发生的信息的授权请求。然后，收单方计算设备520利用发行方计算设备514处理授权，并将授权结果返回给商家。

[0113] 3DS 2协议(以及3DS协议的后续版本)为持卡人、发行方和商家提供许多益处。它通过一种包含丰富、全面的数据集以进行认证决策的方法来降低未授权交易的风险。对于持卡人而言，无论支付渠道或支付设备如何，它都能提供简单、安全且熟悉的在线认证体验。对于发行方而言，它允许“无阻力”认证，其中不需要也不执行显式持卡人升级认证。这样可以实现更智能的风险评估决策，并能够根据需要选择性地质询持卡人。这也改善了持卡人的体验并且提高了整体持卡人对发行方的忠诚度。对于商家而言，3DS 2协议减少了所有经过认证的交易的欺诈，并且通过减少阻力和减少购物车放弃(即，持卡人在已经选择了要购买的一个或多个商品后决定不完成交易)而增加了收入潜力，尤其是对于移动支付渠道。这也改善了持卡人的体验并且提高了整体持卡人对商家的忠诚度。

[0114] 使用3DS 2协议(或3DS协议的后续版本)，支付网络在其品牌上的所有卡上全局地看到100％的所有认证请求。包括发行方和ACS提供者在内的任何其他方都无法提供这种全局可见性。可以利用这种全局可见性来代表发行方提供一致的、基于标准的交易风险分析，从而实现全市场的基于风险的认证方法。

[0115] 与先前的认证方法(例如，3DS 1.0)相比，3DS 2协议(以及3DS协议的后续版本)允许收集、分析和利用大约十倍的交易数据量以防止欺诈。3DS协议中包括的附加数据增加了商家和发行方之间的数据交换，并改善了基于风险的认证(RBA)决策。RBA允许发行方通过交易风险分析检查每个认证请求，同时将防欺诈工作聚焦于防止最大风险的交易。此外，RBA利用行为输入和交易输入二者结合风险引擎来确定交易的风险。

[0116] 被认为安全或低风险的交易被静默地认证(即，所谓的“无阻力”认证)，而较高风险交易受到升级认证。当低风险交易被静默地认证时，已经收集了足够多的数据，以至于进一步的认证几乎没有增加任何价值。因此，RBA有效地取代了对于每笔交易都与持卡人进行显式交互的需要，但交易仍然完全通过认证，责任由发行方承担。因此，在对持卡人最小干扰的情况下完成了更多的交易，有助于电子商务的增长。

[0117] RBA的一个目标是最小化需要主动(即，升级)认证的交易的数量，同时将欺诈保持在最小并且改善交易过程期间的消费者阻力点。利用RBA，收集的信息使得能够进行交易评分并且将交易分类分为低风险、中风险和高风险，允许发行方和ACS 512采取适当的措施。

[0118] 3DS 2协议(以及3DS协议的后续版本)实现了到达目录服务器510的所有交易的全市场级别风险分析。可以使用3DS 2协议(以及3DS协议的后续版本)基于可用的全局数据对

每个交易进行评分和/或标记。另外，操作目录服务器510的支付处理者具有查看跨数字和物理域的持卡人活动的能力，并且可以利用该扩展视角来改进评分。相反，传统的认证服务提供者可能只处理数字域。例如，支付处理者可以指示特定设备是否与欺诈相关联，并且在将来的交易中为发行方标记该设备。然后，发行方可以拒绝涉及该设备的交易或者提示进行附加认证(例如，通过双因素认证)。

[0119] 下面的表2列出了在3DS 2协议中用于认证的多个数据元素。例如，这些数据元素中的至少一些可以包括在发送到目录服务器510的AReq中包括的认证数据中。也作为表示3DS 1.0协议的一部分的十八个数据元素在表2中以粗体表示。本领域技术人员将理解，丰富的数据元素的数量可增长到超出下面列出的这些(例如，在3DS协议的未来版本中)，并且可以包括超过一百七十个数据元素。此外，基于应用的交易(例如，使用移动计算设备执行)可以提供比基于浏览器的交易更多的数据元素。此外，使用Android设备执行的交易可具有超过一百三十个附加元素。

[0120]

	数据元素
1	3DS 请求者认证信息
2	3DS 请求者质询指示符
3	3DS 请求者 ID
4	3DS 请求者发起指示符
5	3DS 请求者名称
6	3DS 请求者非支付认证指示符
7	3DS 请求者交易前认证信息
8	3DS 请求者 URL
9	3DS 服务器操作者 ID
10	3DS 服务器参考号码
11	3DS 服务器交易 ID
12	3DS 服务器 URL
13	账户类型
14	**收单方 BIN**
15	**收单方商家 ID**
16	ACS 指令质询指示符
17	ACS 柜台 ACS 至 SDK
18	**ACS HTML**
19	ACS 操作者 ID
20	ACS 参考号码
21	ACS 呈现类型
22	**ACS 签名内容**
23	ACS 交易 ID

[0121]

	数据元素
24	ACS UI 类型
25	地址匹配指示
26	认证方法
27	认证类型
28	**认证值**
29	浏览器接受头部
30	浏览器 IP 地址
31	浏览器 Java 可用
32	浏览器语言
33	浏览器屏幕色深
34	浏览器屏幕高度
35	浏览器屏幕宽度
36	浏览器时区
37	浏览器用户代理
38	卡/令牌有效日期
39	持卡人账户标识符
40	持卡人账户信息
41	**持卡人账号**
42	持卡人账单地址 城市
43	持卡人账单地址 国家
44	持卡人账单地址 行 1
45	持卡人账单地址 行 2
46	持卡人账单地址 行 3
47	持卡人账单地址 邮政编码
48	持卡人账单地址 州
49	持卡人电子邮件地址
50	持卡人家庭电话号码
51	持卡人移动电话号码
52	持卡人姓名
53	持卡人配送地址 城市
54	持卡人配送地址 国家
55	持卡人配送地址 行 1
56	持卡人配送地址 行 2
57	持卡人配送地址 行 3
58	持卡人配送地址 邮政编码
59	持卡人配送地址 州
60	持卡人工作电话号码
61	质询附加信息文本
62	质询取消指示符
63	质询数据入口
64	质询 HTML 数据入口
65	质询信息头部

[0122]

	数据元素
66	质询信息标记
67	质询信息文本
68	质询信息文本指示符
69	质询选择信息
70	质询窗口大小
71	设备信道
72	设备信息
73	支持的设备呈现选项
74	DS 参考号码
75	DS 交易 ID
76	DS URL
77	电子商务指示
78	EMV 支付令牌指示符
79	可扩展信息 标记 1
80	可扩展信息文本 1
81	分期付款支付数据
82	交互柜台
83	发行方图像
84	商家类别代码
85	**商家国家代码**
86	**商家名称**
87	商家风险指示符
88	消息类别
89	**消息扩展**
90	**消息类型**
91	**消息版本号**
92	通知 URL
93	OOB 应用标记
94	OOB 应用 URL
95	OOB 继续指示符
96	OOB 继续标签
97	支付系统图像
98	**购买账户**
99	**购买**
100	**购买货币指数**
101	**购买日期&时间**
102	**循环的到期**
103	**循环频率**
104	再发质询信息代码
105	再发信息标签
106	结果消息状态
107	SDK 应用 ID

[0123]

	数据元素
108	SDK 柜台 SDK 至 ACS
109	SDK 加密数据
110	SDK 临时公钥 (Qc)
111	SDK 参考号码
112	SDK 交易 ID
113	提交认证标记
114	**交易状态**
115	交易状态理由
116	交易类型
117	原因信息标签
118	原因信息文本

[0124] 表2

[0125] 如上所述，在图5所示的实施例中，ACS 512使用RBA能力执行认证。但是，许多作为发行方处理者用于认证的ACS提供者没有RBA功能。此外，具有RBA能力的ACS提供者可能暂时失去这些能力(例如，由于设备故障)。鉴于3DS 2协议(以及3DS协议的后续版本)的上述优点，与具有此功能的其他ACS提供者相比，没有RBA功能的ACS提供者可能会失去消费者。因此，期望为不具有RBA能力的ACS提供者促进3DS 2协议(以及3DS协议的后续版本)认证。

[0126] 图6是示出另一示例认证系统600中的交易流的示意图，其使用3DS 2协议(或3DS协议的后续版本)进行认证，并且代表不能执行RBA的ACS提供者执行RBA。除非另外指出，否则认证系统600的组件基本上类似于认证系统500(图5中所示)的组件。

[0127] 代替于目录服务器510，认证系统600包括通信地耦合到RBA引擎612(其可以统称为认证平台614)的启用RBA的目录服务器610。启用RBA的目录服务器610和RBA引擎612有助于代表ACS提供者执行RBA，如本文所述。启用RBA的目录服务器610和RBA引擎612可以例如通过交换网络28(图1中所示)来操作。在一些实施例中，认证平台614类似于RBA平台34(图1中示出)和认证服务器112(图2中示出)。

[0128] 如在认证系统500中，启用RBA的目录服务器610从3DS服务器506接收AReq消息。然而，代替于立即将AReq消息转发到ACS512，启用RBA的目录服务器610将AReq消息中的至少一些数据(例如，认证数据)发送到RBA引擎612。

[0129] 在示例实施例中，RBA引擎612分析AReq消息中的数据以生成RBA结果数据。例如，RBA引擎612可以将AReq消息中的数据与一个或多个长期变量(“LTV”)进行比较。一个或多个LTV可以包括与所讨论的PAN相关联的历史认证数据、与PAN相关联的历史授权数据、与PAN相关联的其他历史数据等。LTV可以与卡存在和卡不存在的历史交易二者相关联。例如，LTV可以包括持卡人配送地址、持卡人账单地址、持卡人电子邮件地址、持卡人电话号码、商家名称、商家类别、商家位置和/或至少一个与环境相关的变量(例如，设备细节、浏览器细节)，包括设备ID、IP地址、设备信道等。此外，LTV可以存储在RBA引擎612可访问的数据库中并由交换网络28操作。在一些实施例中，LTV数据将在存储之前被散列化以保护此个人身份信息的安全性。

[0130] 此外，还可以将AReq消息中的数据与其他参数进行比较。例如，为了监视一致性和行为的变化，可以将数据与短期(例如，分钟、小时或天量级)PAN速度和比率进行比较，包括

PAN授权和认证的速度和比率。这可以包括与最近的交易频率、花费的金额、拒绝、历史风险分数等进行比较。替代地，可以使用任何合适的技术来分析AReq消息中的数据以生成RBA结果数据，如本文所述的。

[0131] 在示例实施例中，由RBA引擎612生成的RBA结果数据包括风险分数、风险分析和至少一个原因代码。风险分数是表示所确定的交易的风险的分数，其中较低分数指示较低风险，并且较高分数指示较高风险。换句话说，风险分数表示可疑持卡人(例如，试图进行交易的人)是具有使用支付卡执行支付交易的特权的合法持卡人的可能性。例如，风险分数可以由来自0-999的数字表示和/或由来自0-19的风险阈值类别表示。在一些实施例中，将诸如通过一个或多个消息的授权字段来共享的风险评估将以0-9的等级被量化。本领域技术人员将理解，可以使用任何合适的风险分数。

[0132] 风险分析是对与风险分数对应的风险等级的描述(例如，低风险、中等风险或高风险)。此外，原因代码包括影响风险分数的一个或多个因素。RBA引擎612将RBA结果数据发送到启用RBA的目录服务器610。

[0133] 在一些实施例中，基于多个原因代码类别和相关联的锚来生成原因代码。具体地，建立不同的类别，并且每个类别与多个可激活的锚相关联，如本文所描述的。基于对AReq消息中的数据的分析，RBA引擎612可以激活一个或多个锚。然后基于哪些锚(以及多少锚)被激活来生成原因代码。在一些实施例中，原因代码受规则和/或规则和模型的组合的影响。

[0134] 例如，在一个实施例中，建立三个风险代码类别：持卡人、商家和环境。在此示例中，持卡人类别与五个锚(配送地址、PAN、账单地址、电子邮件和电话)相关联，商家类别与三个锚(商家名称、商家类别和商家国家)相关联，并且环境类别与三个锚(设备信息、IP地址和设备通道)相关联。本领域技术人员将理解，可以建立附加的和/或替代的锚。

[0135] 基于对AReq消息中的数据的分析，RBA引擎612可以激活至少一个锚。例如，对于持卡人类别，如果RBA引擎612确定交易的配送地址已经在过去的交易中与PAN一起被使用和/或配送地址与先前的交易没有变化，则RBA引擎612可以激活配送地址锚。此外，如果PAN在过去的交易中已经具有成功的认证，则RBA引擎612可以激活持卡人类别的PAN锚。

[0136] 对于商家类别，可以基于商家的欺诈率、商家的拒绝率以及商家的未清算的交易率来激活一个或多个锚。此外，当RBA引擎612确定交易的商家类别和商家位置与该商家的历史交易一致时，可以激活一个或多个锚。

[0137] 对于环境类别，如果IP地址已知并且不在“坏”IP地址列表上，则可以激活IP地址锚。此外，如果设备已知并且不在“坏”设备列表上、设备在过去的交易中已经具有成功认证、和/或设备在过去的交易中得分良好，则设备锚可以被激活。

[0138] 以下是用于激活不同类别的锚的标准的一些附加示例。在一个示例中，如果在过去的交易中配送地址已经与PAN一起被使用、配送地址与存档的账单地址相同、配送地址不在“坏”配送地址的列表上以及配送地址与先前的交易没有变化，则配送地址锚被激活。在第二示例中，当配送地址与先前的交易一致、账单地址与之前的交易一致、PAN与持卡人有历史正面关联并且购买金额、日期和时间与之前的交易一致时，配送地址锚、账单地址锚和PAN锚(即，持卡人类别的所有锚)被激活。在第三示例中，当持卡人的联系信息与之前的交易一致、持卡人是可信的持卡人、商家是可信的商家并且PAN在商家处显示已建立的活动和认证历史时，激活持卡人类别和商家类别两者的锚。本领域技术人员将理解，可以基于任何

合适的条件来激活锚。

[0139] 原因代码基于激活的锚生成，并且基于不同类别中的锚之间的连接以分层的顺序被松散地结构化。例如，如果激活持卡人类别中的至少一个锚，则生成正面原因代码(即，指示相对低的风险)。相反，如果激活持卡人类别中的至少一个锚并且还激活商家类别中的至少一个锚，则生成与这两个类别相关的更强的正面原因代码。类似地，如果激活持卡人类别中的至少一个锚，激活商家类别中的至少一个锚，并且激活环境类别中的至少一个锚，则生成与所有三个类别相关的甚至更强的正面原因代码。

[0140] 下面的表3列出了多个示例原因代码。然而，本领域技术人员将理解，根据本文描述的实施例可以利用附加的和/或替代的原因代码。

[0141]

代码	原因代码名称	描述和评注
A	风险事件-可疑的账户活动	商家或支付网络已经检测到持卡人的账户的可疑活动
B	风险事件-未知的设备/账户关系	商家或支付网络尚未建立设备和账户治时间的关系
C	风险事件-与欺诈事件相关联的设备或简档信息	用于交易的设备或用户的简档已经与欺诈事件相关联
D	风险事件-对设备或简档信息的近期	用于交易的设备或用户的简档近期已

[0142]

	的高风险改变	经有高风险改变
E	风险事件-对设备或简档信息的近期改变	用于交易的设备或用户的简档近期已经被改变
F	风险事件-与欺诈事件相关联的 PAN	商家或支付网络已经检测到与用于该交易的 PAN 相关联的欺诈
G	新账户或不充足的数据	这是商家的新帐户（或支付网络的新持卡人详细信息）或此持卡人的数据不足
H	商家/收单方：商家（欺诈）风险高（由支付网络评估）	支付网络已确定商家正在提交具有高欺诈率的交易
I	商家/收单方：商家（欺诈）风险低（由支付网络评估）	支付网络已确定商家正在提交欺诈率高于平均值的交易
J	环境：良好/已知 IP	商家或支付网络熟悉发生交易的 IP 地址，并且已经评估它是一个好的、可信的 IP
K	持卡人：账单地址 - 已建立先前历史	商家或支付网络已建立了持卡人与该帐单地址之间的正面关联
L	持卡人：电子邮件地址 – 已建立先前历史	商家或支付网络已建立了持卡人和该电子邮件地址之间的正面关联。
M	持卡人：电话号码 - 已建立先前历史	商家或支付网络已建立了持卡人和该电话号码之间的正面关联。
N	持卡人：配送地址 – 已建立先前历史	商家或支付网络已建立了持卡人和该配送地址之间的正面关联。
O	持卡人：卡号（PAN）行为建立了对当前交易的高度信任	商家或支付网络已基于历史 PAN 行为建立了对交易的高度信任
P	环境：设备已知	商家或支付网络之前已经见过用于交易的设备，但是可能未在设备上建立该帐户
Q	环境：已在设备上建立帐户	商家或支付网络已经见过该设备上的该帐户交易并且已在设备上认证了账户
R	环境：会话 - 可信/正常/无害会话（没有中间人攻击/没有机器人，没有可疑的帐户活动）	商家或支付网络确定会话的质量
S	建立了多于一个持卡人类别锚	商家或支付网络已建立多个持卡人类别锚
T	建立了多于一个商家类别锚	支付网络已建立多个商家类别锚
U	建立了多个环境类别锚	商家或支付网络已建立多个环境类别锚
V	共同发生：持卡人与商家之间已建立联系	商家或支付网络已建立了跨持卡人和商家类别的联系
W	共同发生：持卡人与环境之间已建立联系	商家或支付网络已建立了跨持卡人和环境类别的联系
X	共同发生：商家与环境之间已建立联系	支付网络已建立了跨商家和环境类别的联系

[0143]

Y	建立了所有三个类别	支付网络已建立了跨持卡人、商家和环境类别的联系
Z	最可信的（被保留以供将来使用）	被保留以供将来使用

[0144] 表3

[0145] 在RBA引擎612生成RBA结果数据(包括原因代码)之后，启用RBA的目录服务器610将RBA结果数据嵌入到AReq消息中以生成增强的AReq消息。例如，在一些实施例中，RBA结果数据作为AReq消息的可扩展标记语言(XML)扩展追加到AReq消息。例如，扩展可以具有以下格式：

```
"name": "ACS RBA",
"id": "A000000004-acsRBA",
"criticalityIndicator": "true",
"data": {
```

[0146]

```
"status":"success",
"score":"150",
"decision":"low risk",
"reasonCode1":"Y",
"reasonCode2":"J"}
```

[0147] 其中“score”是风险分数，“decision”是风险分析，“reasonCode1”和“reasonCode2”是原因代码。在示例性实施例中，原因代码各自作为单个字母被发送。在其他实施例中，原因代码可以用不同的方法表示。在一些实施例中，reasonCode2由商家发送以提供商家对交易的评估。可替代地，可以将RBA结果数据嵌入到AReq消息中，以使用任何合适的过程生成增强的AReq消息。

[0148] 然后，将增强的AReq消息从启用RBA的目录服务器610发送到ACS 512。然后，ACS 512分析增强的AReq消息中的RBA结果数据以进行认证决策。也就是说，在示例实施例中，ACS 512可以至少基于风险分数、风险分析和原因代码中的至少一者确定完全认证交易、拒绝对交易的认证或者(例如，通过向持卡人发出升级质询)对该交易执行附加认证。因此，ACS 512不执行RBA分析，但是仍然能够利用该分析的结果(例如，通过使用在它们自己的欺诈分析平台中的结果)做出认证决策，从而通常导致更多的批准以及更少的欺诈。因此，启用RBA的目录服务器610和RBA引擎612代表ACS 512执行RBA分析。在一些实施例中，ACS 512从多个源接收认证数据。

[0149] 在一些实施例中，当所确定的交易风险足够低时，作为生成并向ACS 512发送增强的AReq消息的替代，启用RBA的目录服务器610完全认证交易本身。具体地，当所确定的交易风险足够低时，启用RBA的目录服务器610自动生成指示交易已被完全认证的ARes，并将

ARes消息发送到3DS服务器506。启用RBA的目录服务器610通过将风险分数和风险分析中的至少一个与预定阈值进行比较，确定交易的风险性低。例如，可以由ACS 512指定预定阈值。因此，ACS 512能够控制哪些交易将被完全认证，而无需将所有交易转发到ACS 512。

[0150] 对于低风险交易绕过ACS 512减少了支付网络上的总体消息量。这又释放了网络资源，从而提高了支付网络的传输速度和整体能力。此外，在一些实施例中，启用RBA的目录服务器610确定ACS 512是否可用。在一些情况下，ACS 512可能离线或不可用。如果ACS 512可用，则启用RBA的目录服务器610可以将包括RBA结果数据的增强AReq消息路由到ACS 512。如果ACS 512不可用，则启用RBA的目录服务器610可以执行认证处理。

[0151] 图7是用于代表接入控制服务器(ACS)认证在线用户的示例方法700的流程图。例如，可以使用认证平台614(图6中示出)来实现方法700。方法700包括接收702认证请求消息，该认证请求消息包括认证数据。方法700还包括从认证请求消息中提取704认证数据。方法700还包括：至少部分地基于所提取的认证数据，生成706包括风险分数、风险分析和至少一个原因代码的RBA结果数据。此外，方法700包括将RBA结果数据嵌入708到认证请求消息中以生成增强的认证请求消息。此外，方法700包括将增强的认证请求消息发送710到ACS，以使得ACS能够基于RBA结果数据做出认证决策。

[0152] 图8是用于认证在线用户的另一示例方法800的流程图。例如，可以使用认证平台614(图6中所示)来实现方法800。

[0153] 在示例实施例中，认证平台614接收802包括认证数据的认证请求消息，如本文所述。认证平台614执行804RBA以生成包括风险分数、风险分析和至少一个原因代码的RBA结果数据。风险分数是表示所确定的交易风险的分数，其中较低分数表示较低风险，较高分数表示较高风险。换句话说，风险分数表示可疑持卡人(例如，试图进行交易的人)是具有使用支付卡执行支付交易的特权的合法持卡人的可能性。例如，风险分数可以由来自0-999的数字表示和/或由来自0-19的风险阈值类别表示。在一些实施例中，将诸如通过一个或多个消息的授权字段来共享的风险评估将以0-9的等级被量化。风险分析是对与风险分数对应的风险等级的描述(例如，低风险、中等风险或高风险)。原因代码包括影响风险分数的一个或多个因素。

[0154] 在示例实施例中，认证平台614将RBA结果数据与存储的认证简档进行比较。认证简档包含用于处理认证请求的多个规则。在一些实施例中，认证简档由发行方计算设备514(如图5所示)提供。规则的示例包括但不限于：当ACS 512(如图5所示)不可用时如何继续、要包括在RBA中的信息、风险分数和风险等级的风险等级阈值、决策风险阈值和专门规则(例如所有跨境交易都要提交给ACS 512)。认证简档存储在RBA平台处，并且每当确定风险分数时都可以访问该认证简档。

[0155] 在示例实施例中，认证平台614将RBA结果数据与认证简档进行比较，以确定与认证请求相关联的交易所关联的风险等级。在一些实施例中，认证平台614将风险分数与认证简档中的一个或多个阈值进行比较，以确定与交易相关联的风险等级。在其他实施例中，认证平台614将风险分析、原因代码和/或来自RBA结果数据的数据的任何其他组合以及认证数据中的潜在的一些或所有认证数据与认证简档进行比较，以确定与该交易相关联的风险等级。例如，风险分数为900或更低可被视为低风险，风险分数在900和980之间可被视为中等风险，风险分数高于980可被视为高风险。本领域技术人员将理解，可以使用任何合适的

风险分数阈值和任何数量的风险等级。

[0156] 在示例实施例中，认证平台614确定806风险等级是否为高风险。例如，认证平台614可以确定806交易明显是欺诈性的。在这种情况下，认证平台614使认证失败并拒绝808该交易。在示例实施例中，认证平台614可以拒绝808该交易。认证平台614将包括拒绝的认证响应(ARes)消息发送到3DS服务器506(如图5所示)。3DS服务器506可以向商家发送包括拒绝的ARes消息，其中商家确定是否继续授权过程。在这些实施例中，在商家在接收到拒绝之后开始授权过程的情况下，该交易被认为是仅商家认证，其中商家承担交易的风险。

[0157] 当认证平台614确定交易明显是欺诈性的时，认证平台614拒绝交易而不(例如，向ACS和/或发行方)发送认证数据。具体地，认证平台614使认证失败并将该失败在ARes消息中传送给认证请求者。基于该失败，然后商家不应当提交交易以进行授权，从而终止交易。因此，因为在认证期间(并且在授权之前)拒绝交易，所以不通过支付处理网络发送授权消息。这保护了支付处理网络的安全性，因为支付处理网络永远不会暴露于与欺诈性交易相关联的授权数据。此外，认证平台614可以通知发行方和/或商家该交易明显是欺诈性的，从而使得发行方和/或商家能够采取适当的行动(例如，标记相关联的账户号和/或持卡人)。

[0158] 认证平台614确定810交易是中等风险还是低风险的。如果交易是低风险的，则认证平台614可以批准814交易并将包括批准的认证响应(ARes)消息发送到3DS服务器506，其中3DS服务器506和商家中的至少一个可以发起授权过程。如果交易是中等风险的，则认证平台614可以向持卡人22(图1中示出)发出812升级质询。基于升级质询的结果，认证平台614可以批准或拒绝该交易。在一些实施例中，如果交易是中等风险的，则认证平台614将RBA结果数据发送到ACS 512，使得ACS 512将执行升级质询。在其他实施例中，认证平台614可以在不同风险等级采取不同措施，并且具有用于基于认证简档进行分析的附加的或更少的风险等级。

[0159] 图9是用于认证在线用户的另一示例方法900的流程图。例如，可以使用认证平台614(图6中所示)来实现方法900。方法900包括存储902认证简档。认证简档包含用于处理认证请求的多个规则。方法900还包括接收904认证请求消息，该认证请求消息包括认证数据。方法900还包括从认证请求消息中提取906认证数据。方法900还包括至少部分地基于所提取的认证数据生成908包括风险分数、风险分析和至少一个原因代码的RBA结果数据。此外，方法900包括基于认证简档和RBA结果数据来路由910RBA结果数据。

[0160] 在一些实施例中，认证平台614将RBA结果数据发送到认证请求消息的源，例如3DS服务器506(图5中所示)。例如，在一些实施例中，操作3DS服务器506的商家可以请求和接收RBA结果数据，如本文所述，该RBA结果数据包括风险分数、风险分析和至少一个原因代码。商家可以使用RBA结果数据来更新商家自己的风险模型，并且还可以将RBA结果数据与商家独立生成的风险分析结果进行比较，以确定RBA结果数据是否与商家生成的风险分析结果大体一致。

[0161] 在一些实施例中，认证请求消息与在线支付卡交易相关联。认证简档与发行方银行30(如图1所示)相关联。认证请求消息的源是发行方计算设备514(如图5所示)。因此，在一些实施例中，认证平台614将RBA结果数据直接发送到发行方计算设备514，并与发行方计算设备514一起处理认证。例如，发行方银行30可以向认证平台614登记一定范围的卡号，并请求认证平台614直接与发行方计算设备514一起工作，以便对涉及登记范围中的卡号的交

易进行认证。

[0162] 在一些实施例中，认证平台614确定接入控制服务器(ACS)512(图5中所示)是否可用。如果ACS 512可用，则认证平台614将RBA结果数据嵌入到认证请求消息中以生成增强的认证请求消息。认证平台614将增强的认证请求消息发送到ACS 512，以使得ACS 512能够基于RBA结果数据做出认证决策。如果ACS 512不可用，则认证平台614基于RBA结果数据和认证简档生成认证决策。

[0163] 在一些另外的实施例中，认证平台614基于RBA数据和认证简档来确定风险等级。在这些实施例中的一些实施例中，风险等级至少包括用于与认证请求相关联的交易的低风险、中等风险和高风险。在这些实施例中，如果风险等级低，则认证平台614将认证批准消息发送到3DS服务器506。

[0164] 如果风险是中等的，则认证平台614向在线用户22(图1中示出)发送升级质询。认证平台614从在线用户22接收对升级质询的响应。认证平台614基于对升级质询的响应和RBA结果数据来确定认证决策。在一些其他实施例中，如果风险是中等的，则认证平台614将RBA结果数据发送到ACS 512。ACS 512与在线用户22一起执行升级质询。

[0165] 如果风险高，则认证平台614将认证拒绝消息发送到3DS服务器506。

[0166] 图10是用于代表接入控制服务器(ACS)512(图5中示出)来认证在线用户的另一示例方法1000的流程图。例如，可以使用认证平台614(图6中所示)来实现方法1000。方法1000包括接收1002用于交易的认证请求消息。该认证请求消息包括认证数据。方法1000还包括从认证请求消息中提取1004认证数据。方法1000还包括确定1006ACS 512是否可用于处理交易。如果ACS 512不可用，则该方法包括至少部分地基于所提取的认证数据生成1008基于风险的认证(RBA)结果数据，该RBA结果数据包括风险分数和指示影响了所生成的风险分数的至少一个因素的至少一个原因代码。如果ACS 512不可用，则该方法还包括基于RBA结果数据发送1010认证响应消息。在一些实施例中，认证平台614基于RBA结果数据生成认证决策，并将认证决策嵌入认证响应消息中。

[0167] 在示例实施例中，交易被分类为“仅商家”或“完全认证”。“完全认证”交易通常被认为是已经认证的低风险交易。“仅商家”交易是风险更大的交易。在一些实施例中，“仅商家”交易已被认证。在示例实施例中，认证响应中的一个或多个指示符指示交易是“仅商家”还是“完全认证”的。一个或多个指示符还可以指示是否对于交易尝试了认证。该信息由商家用来确定是否开始交易的授权过程。在一些实施例中，该信息还存储在数据库120中(如图2所示)，并且在授权过程20期间由交换网络28和发行方银行30(均在图1中示出)中的至少一个引用。

[0168] 在示例实施例中，认证平台614对交易执行认证过程，包括RBA。该分析基于机器学习模型，其中随着时间的推移，认证平台614能够提高它确定与交易相关联的风险等级的能力。认证平台614分析由ACS 512认证的交易，并将这些交易与历史数据进行比较，以便为每个发行方银行30生成风险模型。通过比较每个交易中的数据点，风险模型将指示基于相应认证请求中的认证数据的与每个交易相关联的风险量。这允许认证平台614在ACS 512不可用时分析交易，并对这些交易执行认证，以提供对认证请求的响应。因此，认证平台614可以确定所接收的授权请求基本上类似于被ACS 512评分为低风险的先前交易。因此，允许认证平台614以一定程度的确定性来确定所接收的交易是低风险的。

[0169] 在一些实施例中，认证平台614通过将认证请求消息发送到ACS 512来确定ACS 512是否可用。在这些实施例中，认证平台614等待来自ACS 512的响应预定时间段。如果在预定时间段之后没有从ACS 512接收到响应，则认证平台614确定ACS 512不可用。可替代地，认证平台614可以从ACS 512接收指示ACS 512不能执行认证的响应。来自ACS 512的响应可以指示在线用户没有向ACS 512登记，ACS 512当前不可用，或者ACS 512不能认证在线用户。该指示可以包含在来自ACS 512的响应消息中。在其他实施例中，认证平台614可以向ACS 512发送周期性状态检查消息，以确定ACS 512是否可用。

[0170] 在一些实施例中，认证平台614基于提取的认证数据确定在线用户没有与ACS 512相关联。在这些实施例中，与在线用户相关联的发行方尚未向ACS 512注册。在这些实施例中，认证平台614基于RBA结果数据生成认证决策。

[0171] 在一些另外的实施例中，认证平台614确定认证请求消息是否符合3DS 2协议或3DS协议的后续版本。如果认证请求消息不符合适当的3DS协议，则认证平台614绕过确定ACS 512是否可用。在这种情况下，认证平台614发送认证响应消息，该认证响应消息指示该交易被认为是仅商家的并且没有尝试认证。

[0172] 在一些实施例中，认证平台614基于RBA结果数据确定风险等级。如果风险等级低，则认证平台614在认证响应消息中嵌入指示符，该指示符指示该交易是“完全认证的”。如果风险等级不低，则认证平台614在认证响应消息中嵌入一个或多个指示符，该一个或多个指示符指示该交易是仅商家的交易并且尝试了认证。

[0173] 图11A和图11B是示出涉及对与受监管市场相关联的交易的条件SCA评估的附加示例实施例的泳道图。图11A涉及当确定交易具有足够低的风险和低价值时被允许避免监管者施加的SCA升级质询的交易。图11B涉及当交易风险更大或交易价值更高时被迫使进入SCA升级质询的交易。在这样的情况下，涉及启用RBA的目录服务器(或仅“目录服务器”)610和RBA引擎612的上述系统和方法中的任何系统和方法可以与条件SCA一起使用，这受制于这里描述的监管者施加的限制。

[0174] 现在参照图11A，在该示例实施例中，在步骤1110，持卡人22通过其计算设备(此处由3DS客户端502表示)发起与商家(此处由3DS服务器506表示)的在线交易。3DS服务器506在步骤1112生成并向目录服务器610发送AReq消息1102，并从AReq消息中提取交易数据(例如，如上面参考图6所描述的)。AReq消息1102包括交易的交易价值，以及与交易相关联的其他认证数据(例如，作为3DS AReq消息)。目录服务器610接收AReq消息1102并确定该交易涉及由监管实体监管的市场，监管实体诸如(例如，基于持卡人22、商家24、商家银行26或发行方银行30的身份或位置)与交易相关联的特定国家的中央银行。

[0175] 一些受监管市场中的交易可能受到针对所有交易强制的SCA的约束。在示例实施例中，该示例交易的受监管市场已选择如本文所述的条件SCA。在这样的市场中，监管者可以通常对交易强制要求SCA，但可以允许在特定情况下在没有SCA的情况下对交易进行认证。由此，目录服务器610识别该特定受监管市场的条件SCA的交易限制和风险阈值。交易限制表示如下阈值交易价值：如果还满足风险阈值，则在该阈值交易价值以下可以避免SCA。在本文描述的实施例中，交易限制可以是，例如，特定交易的货币价值(例如，2000卢比、30欧元等)、交易的数量(例如，5个无阻力交易)、或累积货币价值(例如，100欧元)。因此，交易限制可以由除交易的货币价值之外的参数来定义。本领域技术人员将理解，可以建立任何

合适类型的交易限制。

[0176] 风险阈值表示(例如,由RBA引擎612确定或“评分”的)与交易相关联的欺诈风险等级。换句话说,并且例如,如果交易的风险等级是“低的”(例如,低于风险分数阈值)并且交易是“低价值”交易(例如,低于交易阈值价值),则受监管实体可以不强制要求SCA。如果交易价值不是低价值交易(例如,等于或高于交易阈值价值)或者如果交易不是低风险交易(例如,等于或高于风险分数阈值),则受监管实体可以强制要求SCA。

[0177] 目录服务器610将交易价值与由监管实体设置的交易限制进行比较,并且在该示例中,确定交易价值小于交易限制(例如,交易是“低价值”交易)。由此,目录服务器610在步骤1114使用RBA引擎612来评估与AReq相关联的风险。如上所述,RBA引擎612使用与AReq相关联的认证数据和其他交易数据来评估与交易相关联的风险。RBA引擎612生成基于风险的认证结果数据,该基于风险的认证结果数据包括交易的风险分数。

[0178] 在该示例中,RBA引擎612将针对该交易生成的风险分数与针对该受监管市场识别的风险阈值进行比较,并确定该交易中的欺诈风险低于风险阈值。在一些实施例中,风险分数和风险阈值可以是整数值,这些整数值可以被比较以确定风险分数是大于还是小于风险阈值。在其他实施例中,风险阈值可以是分级的类别集合中的类别(例如,“低”、“中等”、“高”),并且风险分数可以具有该相同的分级的类别集合,或者风险分数可以是映射到该分级的类别集合中的值(例如,对于每个类别具有监管者定义的范围、发行方定义的范围或系统定义的范围)。例如,RBA引擎612可以允许该市场的监管者将“低风险”类别定义为(例如,如由RBA引擎612依据3DS 2评估的)分数低于400的任何交易。

[0179] 继续该示例,RBA引擎612在步骤1104已经确定交易既“低”又“低于”。换句话说,交易既是低价值交易又低于监管者的交易阈值。因此,就监管者而言,交易不被强制要求执行SCA。但是,某些发行方可能对SCA升级有更严格的要求,或者可能有其他理由不顾SCA升级考虑而拒绝认证。例如,一些发行方可能拒绝被评估为“高”风险的任何CNP交易。为了便于描述,在图11A和图11B中没有明确地示出这样的流和拒绝。相反,图11A和图11B关注涉及当强制要求SCA或允许避免SCA时所涉及的场景。

[0180] 在一些场景中,可以委托认证平台(例如,目录服务器610和RBA引擎612)代表发行方514执行认证处理。在其他场景中,认证可以由ACS 512执行。因此,在测试1116,如果认证平台代表发行方514进行认证,则RBA引擎612在步骤1118生成批准该交易的ARes消息1106(假设没有对于认证拒绝的其他原因)并且在步骤1120将ARes 1106发送到3DS服务器506,而无需针对消费者22执行SCA升级认证。

[0181] 如果在测试1116处,认证平台不代表发行方514执行认证(例如,发行方514使ACS 512执行认证服务),则RBA引擎612在步骤1122将增强的AReq消息1108发送到ACS 512。除了与3DS 2相关联的上文描述的附加RBA数据之外,增强AReq还可以包括数据字段,该数据字段指示SCA升级不是由该交易的所涉及的(一个或多个)市场强制要求的。然而,发行方514或ACS 512可以以其他方式确定对交易执行SCA(例如,如果发行方对某些类型的交易优选这样或出于其他考虑因素)。如果在测试1130,ACS 512没有提示SCA升级,则ACS 512在步骤1134向认证平台返回ARes消息1132,以批准对交易的认证。

[0182] 如果在测试1130,ACS 512确定提示SCA升级,则ACS 512在步骤1136经由3DS服务器506(或3DS客户端502)提示升级1138。消费者22将升级输入1142提供回到3DS服务器506

(或直接提供到ACS 512),并且在成功升级后,ACS 512在步骤1146将ARes消息1132发送到认证服务。

[0183] 现在参考图11B,在该示例中,认证平台确定交易不满足避免SCA升级的要求,并且因此强制要求SCA升级。在示例实施例中,RBA引擎612在步骤1150确定交易价值高于由监管实体设置的交易限制,或确定交易风险不满足由监管实体设置的风险阈值,或确定这两者。如果在测试1152,认证平台代表发行方514,并且假设没有拒绝交易的认证的其他理由,则RBA引擎612在步骤1154提示消费者22的升级1156。消费者22在步骤1140直接与目录服务器610或在步骤1158经由3DS服务器506用升级输入1142响应,并且在成功的升级质询后,3DS服务器506将ARes消息1106发送到3DS服务器506,从而批准对交易的认证。

[0184] 如果在测试1152,ACS 512代表发行方514,则RBA引擎612在步骤1154发送增强的AReq 1108(此处由1162表示)以及迫使对于该交易进行消费者22的SCA升级质询的指示。除了与3DS 2相关联的上述附加RBA数据之外,增强的AReq还可以包括数据字段,该数据字段强制要求ACS 512对该交易执行SCA升级(例如,如果以其他方式认为该交易被批准由ACS 512进行认证)。换句话说,AReq 1108用于通知ACS 512在没有SCA的情况下不可以认证该交易。假设没有拒绝对交易的认证的其他理由,ACS 512识别该交易经受强制要求的SCA升级并在步骤1136、1140、1144中提示升级1138,并且在步骤1146和1120中发送批准该交易的ARes 1132,如上所述。

[0185] 在一些实施例中,认证平台提供由监管者使用的图形用户界面(GUI)控制面板(未示出)。例如,GUI可以允许监管者查看和评估与它们的市场相关联的欺诈数据。例如,在一个实施例中,GUI控制面板可以被配置为显示历史欺诈数据,该历史欺诈数据指示当满足由监管实体设置的风险阈值和交易限制时不被强制要求由RBA引擎612用SCA认证的交易中存在的欺诈等级(例如,RBA内的“无阻力交易”的百分比,可能包括批准率或欺诈基点)。在一个实施例中,GUI控制面板可以被配置为显示历史欺诈数据,该历史欺诈数据指示在当不满足风险阈值或交易限制中的一个或多个时被强制要求由RBA引擎612用SCA认证的交易中存在的欺诈等级(例如,在RBA内升级的交易百分比,可能以及升级的类型、批准率、欺诈基点)。这样的数据可以包括电子总美元价值(eGDV)、电子交易计数或这样的指标随时间的增长。这样的数据还可以按通道呈现。例如,这样的数据可以限于移动设备交易、基于浏览器的交易、电话交易和邮件交易。由此,GUI可以允许监管者确定它们的当前设置如何影响这些类型的交易中的欺诈。

[0186] 在一些实施例中,GUI允许监管者调整与它们的市场相关联的条件SCA设置。例如,GUI可以允许监管着更改避免SCA所需的风险阈值,或者更改可以避免SCA的交易的交易限制。在一些实施例中,GUI提供对条件SCA设置的预期改变的模拟分析。例如,通过使用历史数据,GUI可以提供对提议的较高风险阈值或对提议的较高交易限制的欺诈影响分析,可能是估计在所提议的设置下的预测欺诈等级。因此,GUI可以允许监管者基于预期变化确定潜在影响或潜在结果。

[0187] 图12是用于增加批准、减少欺诈和改善消费者体验的改进的认证过程1200的流程图。例如,可以使用本文描述的系统和方法来实现认证过程1200。如图12所示,认证数据1202通过智能接口1204发送到认证平台1206(例如认证平台614)。如上所述,与先前的认证方法(例如,3DS 1.0)相比,3DS 2协议(以及3DS协议的后续版本)下的认证数据1202包括要

收集、分析和利用以防止欺诈的大约十倍的交易数据量。通过使用认证数据1202，认证平台1206执行(如本文所述的)智能认证1208以生成RBA结果数据。决策智能(DI)1210使用其他数据源(即，单独的模型)来影响授权决策。在一些实施例中，RBA结果数据可以合并到DI 1210中。这些评估使得利益相关方1212(例如，ACS、商家和/或发行方)能够完成交易的认证(和认证)。

[0188] 认证过程1200使得能够将在线用户认证为支付账户的合法用户，而不必(例如，作为升级质询的一部分)询问用户的附加问题或者不必请求来自用户的附加输入。因此，认证过程1200评估欺诈风险，而不会针对用户产生可能导致用户终止交易的任何附加阻力。

[0189] 处理器或处理元件可以采用人工智能和/或使用有监督或无监督机器学习进行训练，并且机器学习程序可以采用神经网络，该神经网络可以是卷积神经网络、深度学习神经网络、或者在两个或更多个感兴趣的领域或范畴中学习的组合学习模块或程序。机器学习可以涉及识别和认识现有数据中的模式，以便于促进对后续数据进行预测。可以基于示例输入来创建模型，以便对新输入进行有效且可靠的预测。

[0190] 附加地或可替代地，可以通过将样本数据集或某些数据(诸如图像数据、文本数据、报告数据和/或数值分析)输入到程序中来训练机器学习程序。机器学习程序可以利用深度学习算法，深度学习算法可以主要关注模式识别，并且可以在处理多个示例之后被训练。机器学习程序可以单独地或组合地包括贝叶斯程序学习(BPL)、语音识别和合成、图像或对象识别、光学字符识别和/或自然语言处理。机器学习程序还可以包括自然语言处理、语义分析、自动推理和/或机器学习。

[0191] 在有监督机器学习中，可以向处理元件提供示例输入和与示例输入相关联的输出，并且可以寻求发现将输入映射到输出的一般规则，使得当提供后续的新输入时，处理元件可以基于所发现的规则来准确预测正确的输出。在无监督的机器学习中，处理元件可能需要在未标记的示例输入中找到它自己的结构。在一个实施例中，机器学习技术可用于提取关于计算机设备、计算机设备的用户、托管计算机设备的计算机网络、在计算机设备上执行的服务的数据和/或其他数据。

[0192] 基于这些分析，处理元件可以学习如何识别随后可以应用于训练模型、分析交易和认证数据以及检测和分析风险的特性和模式。

[0193] 如本文所使用的，术语“非态计算机可读介质”旨在表示以用于信息(诸如计算机可读指令、数据结构、程序模块和子模块或任何设备中的其他数据)的短期和长期存储的任何方法或技术实现的任何有形的基于计算机的设备。因此，本文描述的方法可以被编码为体现在有形的、非暂态的计算机可读介质中的可执行指令，该计算机可读介质包括但不限于存储设备和/或存储器设备。当由处理器执行时，这些指令使处理器执行本文描述的方法的至少一部分。此外，如本文所使用的，术语“非暂态计算机可读介质”包括所有有形的计算机可读介质，包括但不限于非暂态计算机存储设备，非暂态计算机存储设备包括但不限于易失性和非易失性介质以及可移除的和不可移除的介质，诸如固件、物理和虚拟存储装置、CD-ROM、DVD以及诸如网络或互联网之类的任何其他数字源、以及尚未开发的数字装置，除了暂态的、传播的信号是唯一的例外。

[0194] 该书面描述使用示例来公开本公开(包括最佳模式)，并且还使得本领域技术人员能够实践实施例，包括制造和使用任何设备或系统以及执行任何结合的处理。本公开的可

专利范围由权利要求限定，并且可以包括本领域技术人员想到的其它示例。如果这些其它示例具有与权利要求的字面语言并无不同的结构元素，或者如果它们包括与权利要求的字面语言无实质差别的等效结构元素，则这些其它示例旨在落入权利要求的范围内。

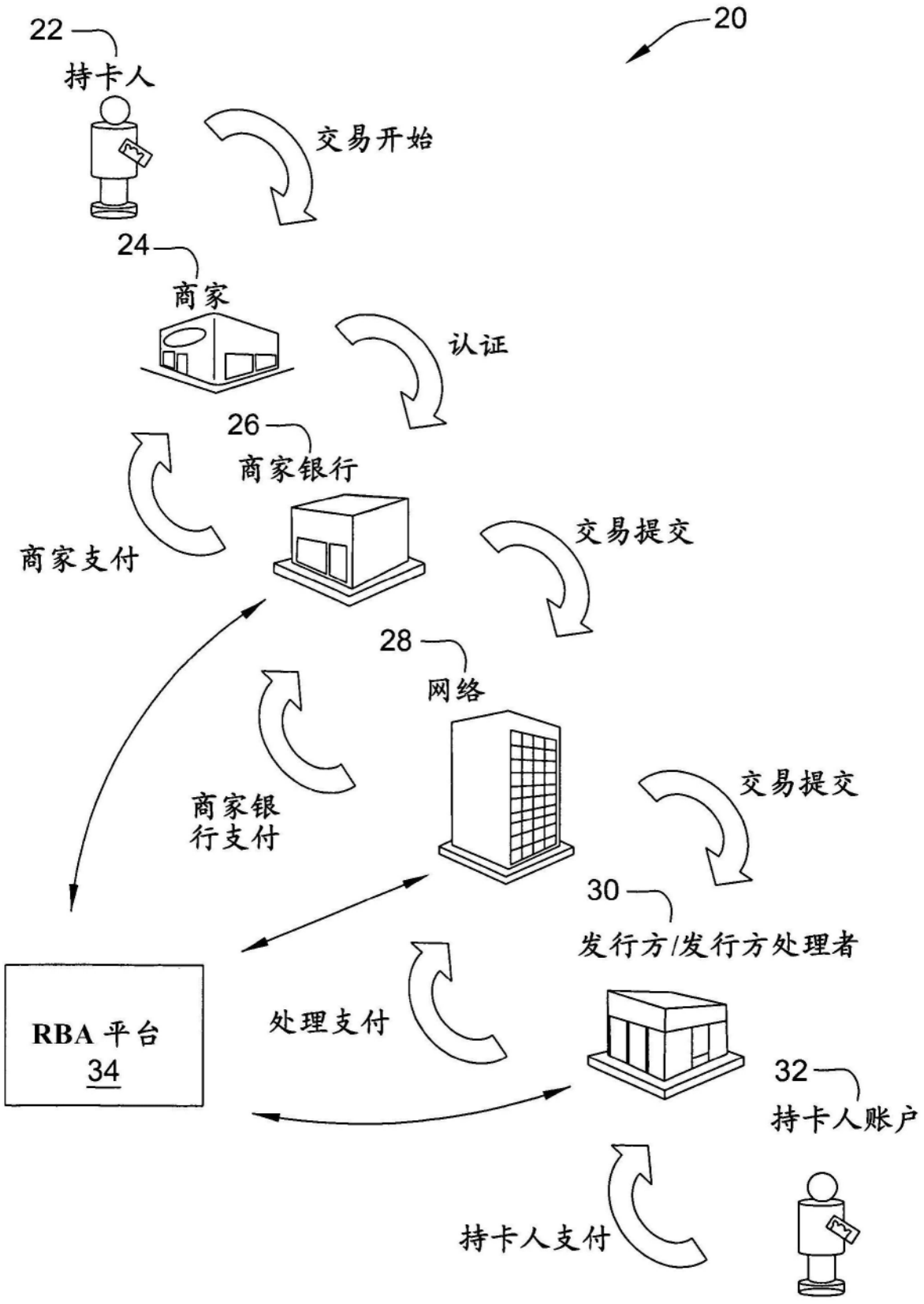

20
22
持卡人
交易开始
24
商家
认证
26
商家银行
商家支付
交易提交
28
网络
商家银行支付
交易提交
30
发行方/发行方处理者
RBA 平台
34
处理支付
32
持卡人账户
持卡人支付

图1

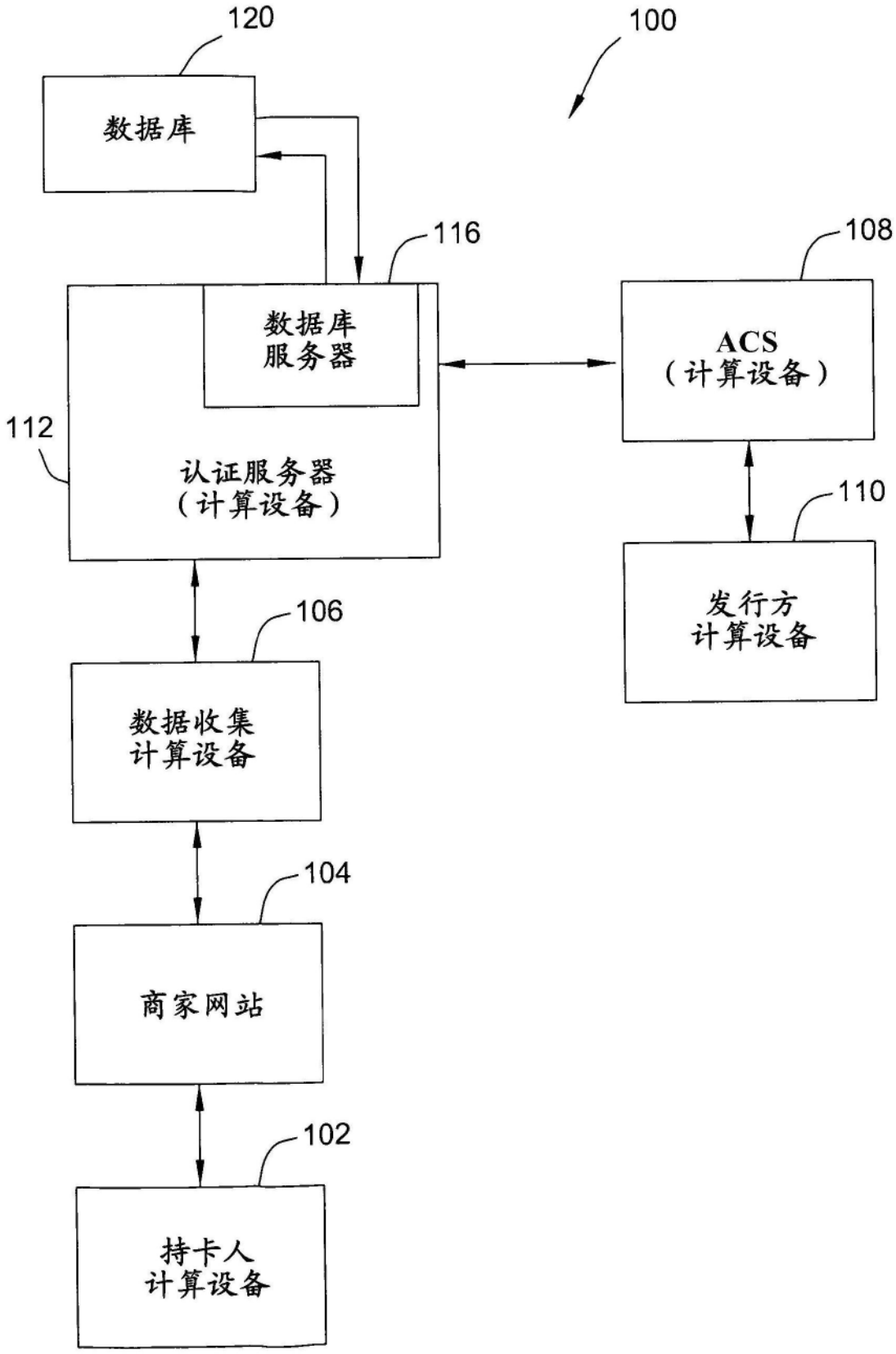

120
100
数据库
116
108
数据库
服务器
ACS
（计算设备）
112
认证服务器
（计算设备）
110
发行方
计算设备
106
数据收集
计算设备
104
商家网站
102
持卡人
计算设备

图2

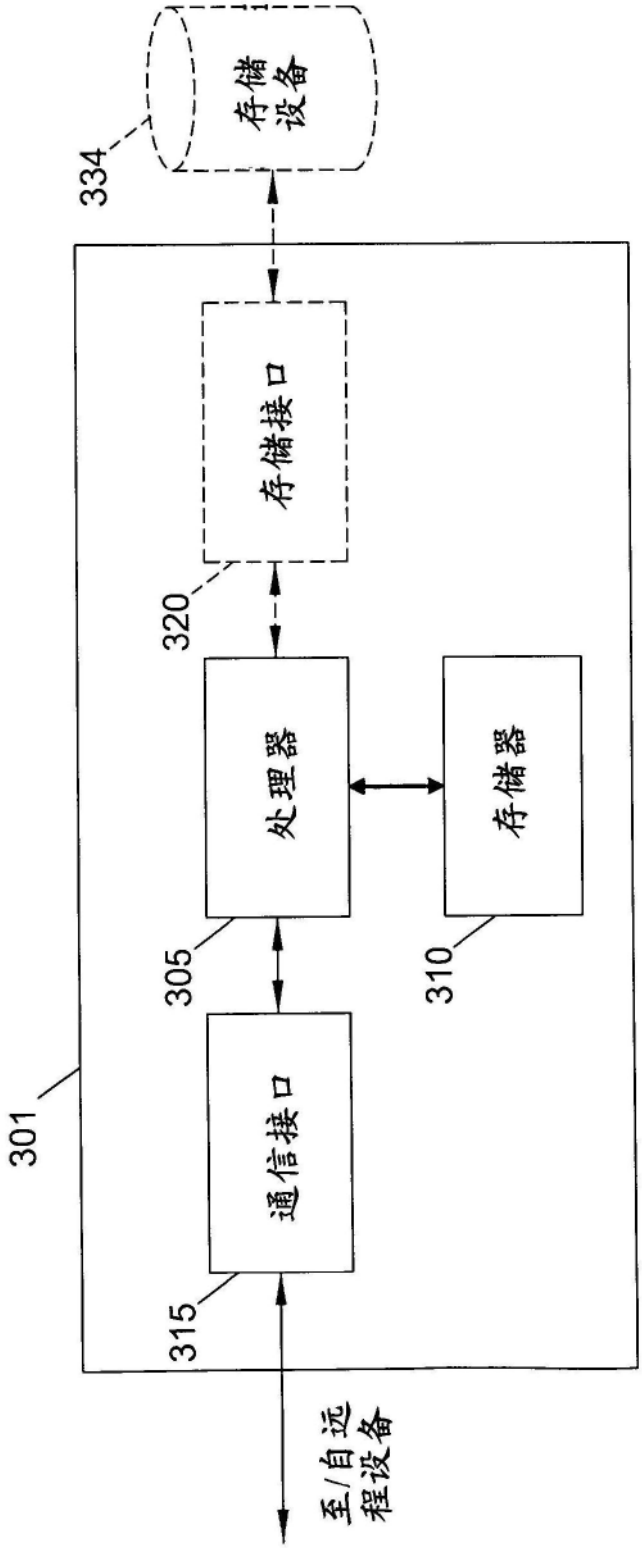


图3

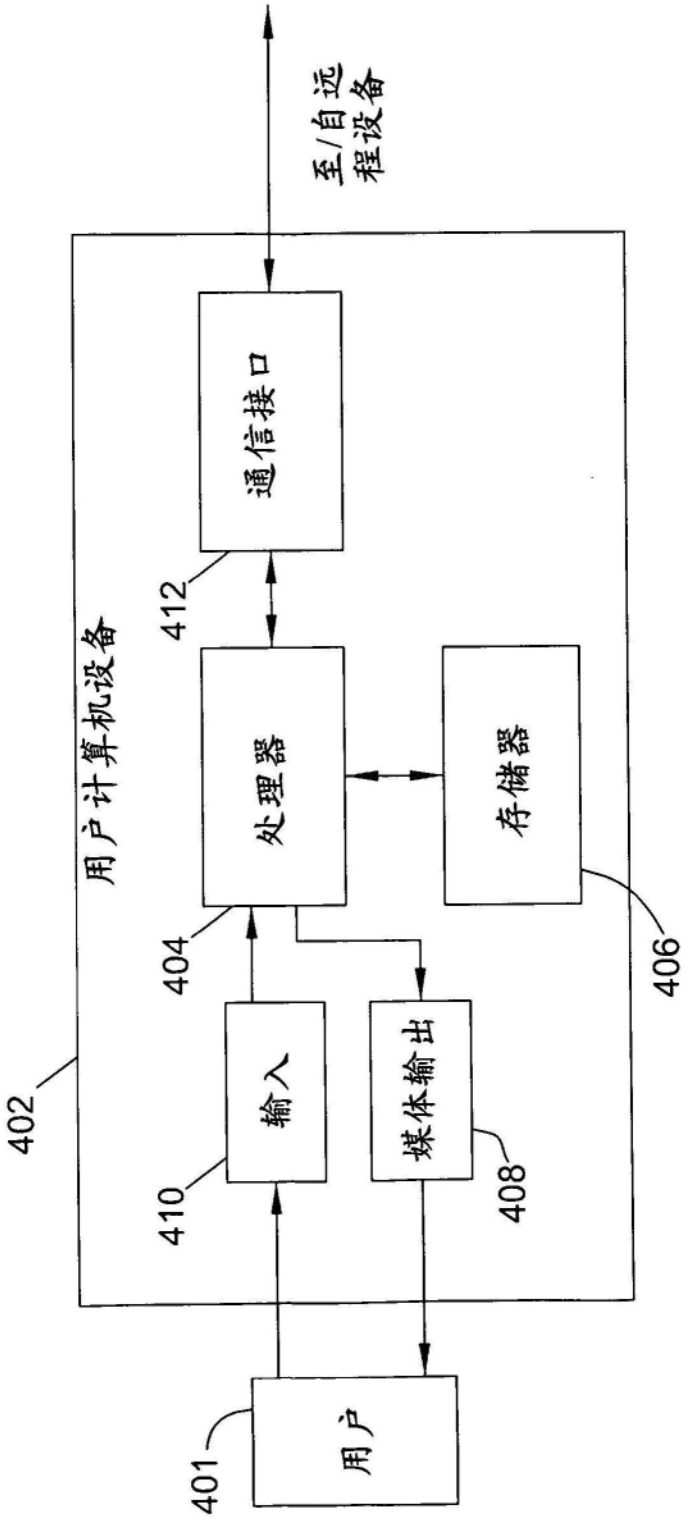

至/自远程设备
通信接口
412
用户计算机设备
处理器
存储器
404
406
402
输入
媒体输出
410
408
用户
401

图4

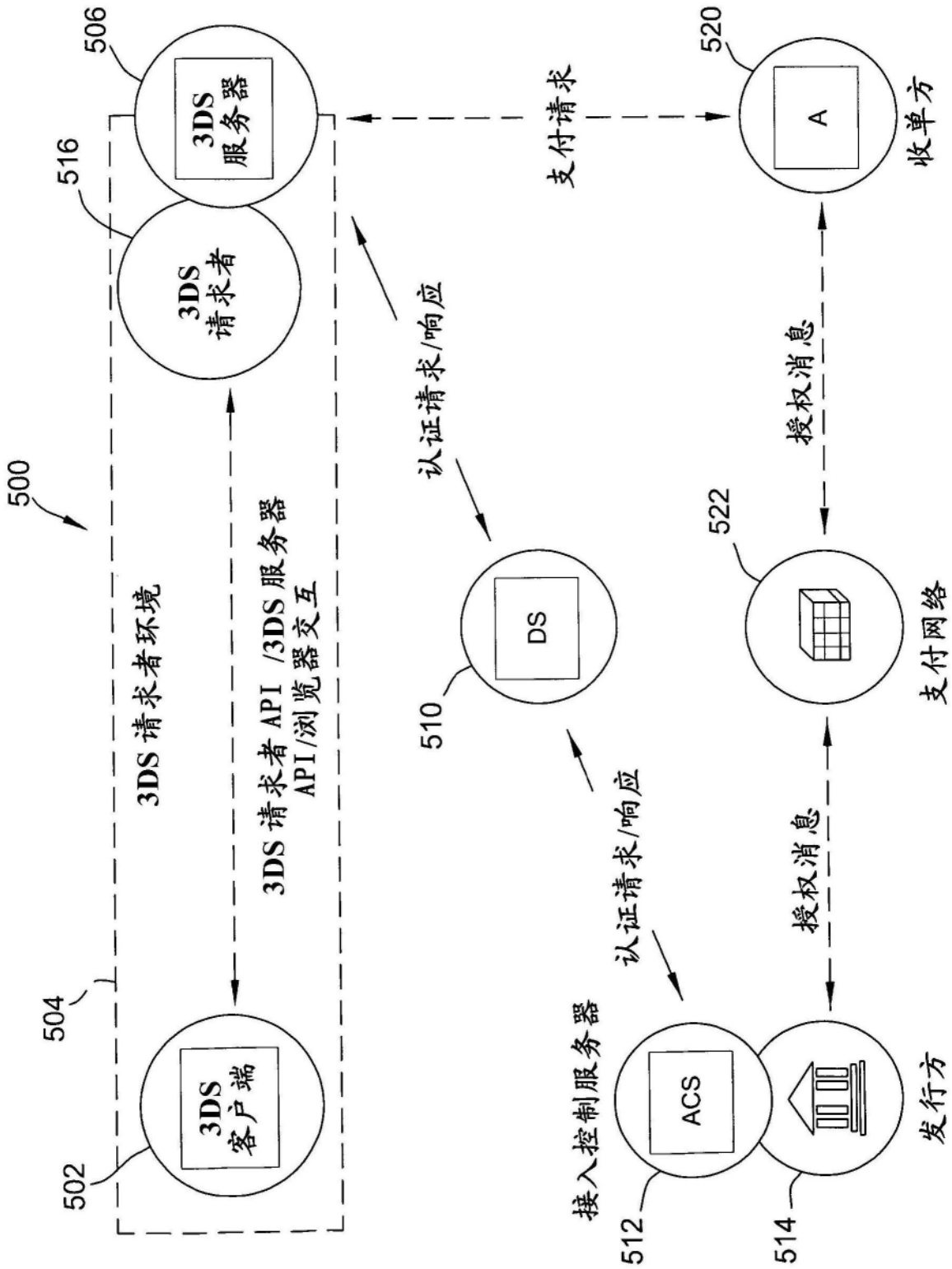

500
3DS 请求者环境
3DS 请求者 API /3DS 服务器 API/浏览器交互
504
502
3DS 客户端
516
3DS 请求者
506
3DS 服务器
认证请求/响应
支付请求
520
A
收单方
授权消息
522
支付网络
510
DS
接入控制服务器
认证请求/响应
ACS
512
授权消息
514
发行方

图5

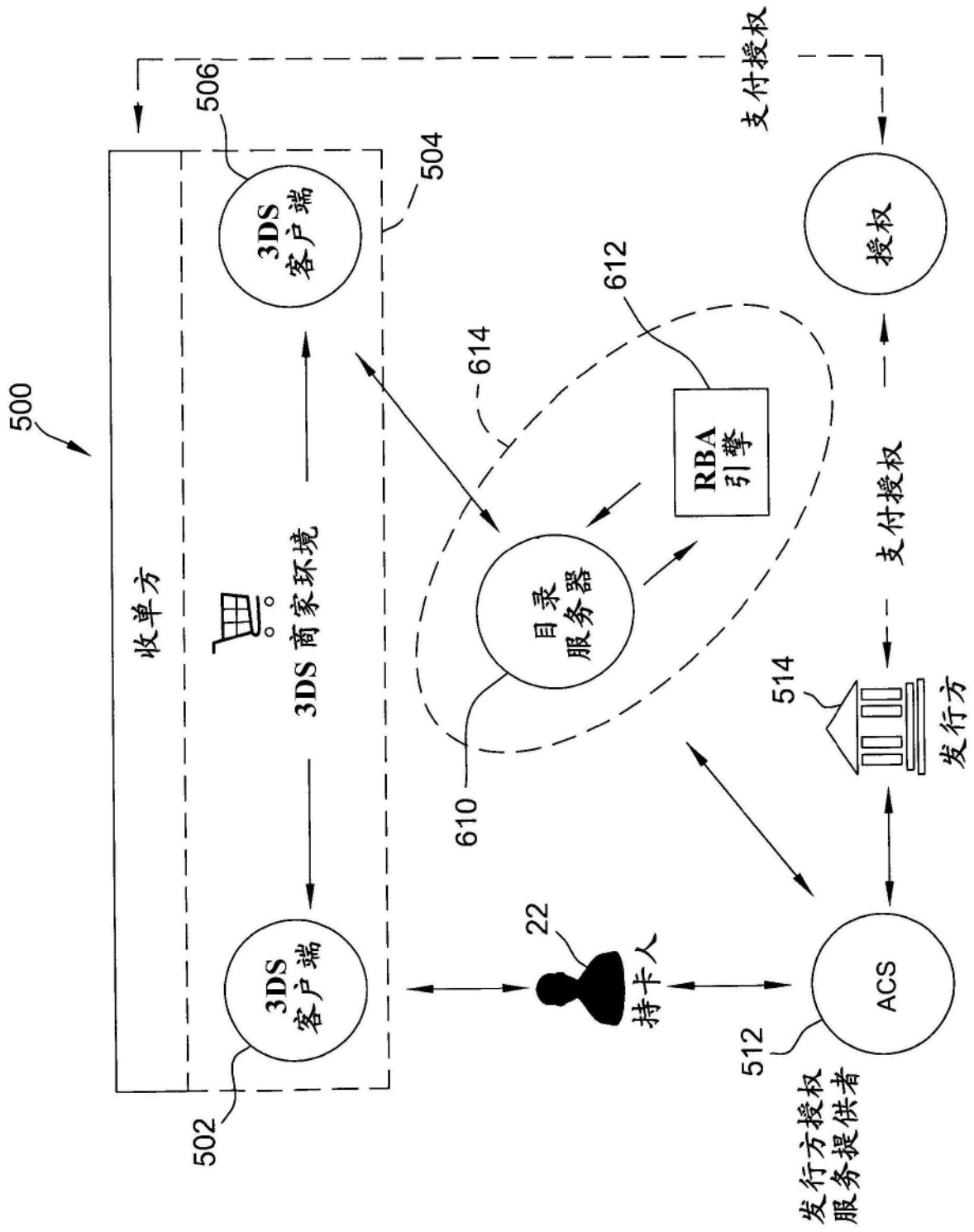

500
收单方
506
504
3DS
客户端
3DS 商家环境
3DS
客户端
502
22
持卡人
512
ACS
发行方授权
服务提供者
610
目录
服务器
614
612
RBA
引擎
514
发行方
支付授权
授权
支付授权

图6

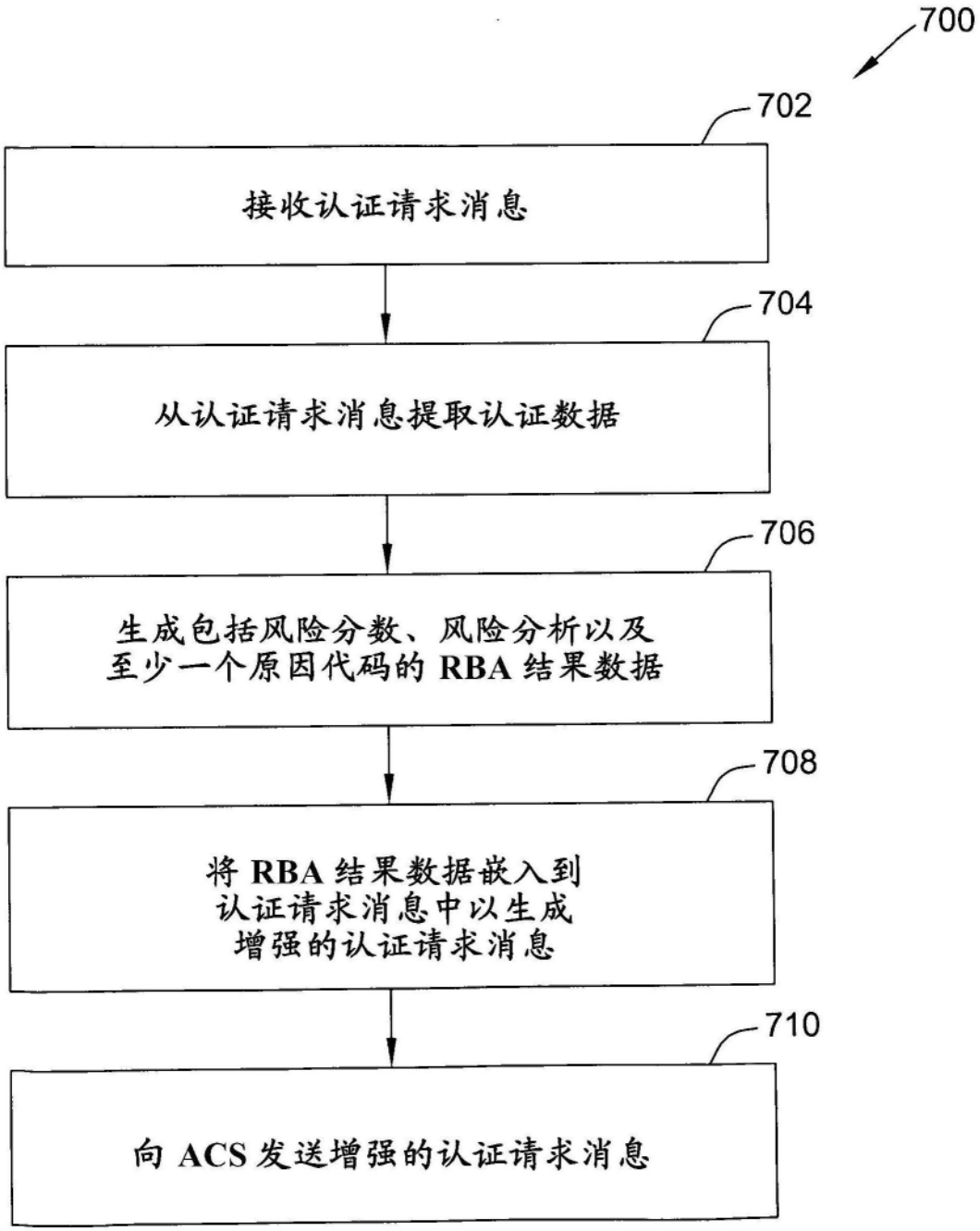

700
702
接收认证请求消息
704
从认证请求消息提取认证数据
706
生成包括风险分数、风险分析以及
至少一个原因代码的 RBA 结果数据
708
将 RBA 结果数据嵌入到
认证请求消息中以生成
增强的认证请求消息
710
向 ACS 发送增强的认证请求消息

图7

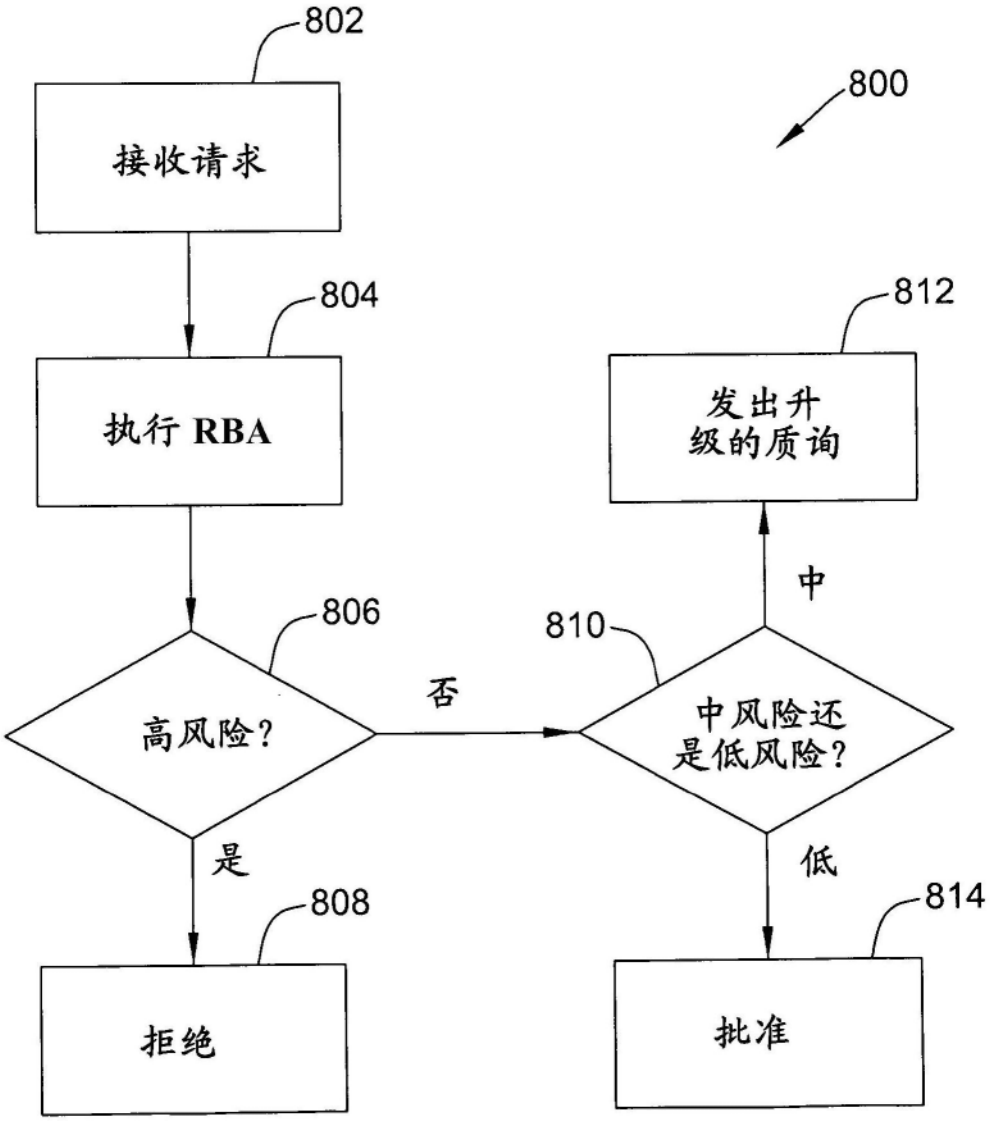

802
接收请求
800
804
执行 RBA
812
发出升级的质询
806
高风险?
否
810
中风险还是低风险?
中
是
低
808
拒绝
814
批准

图8

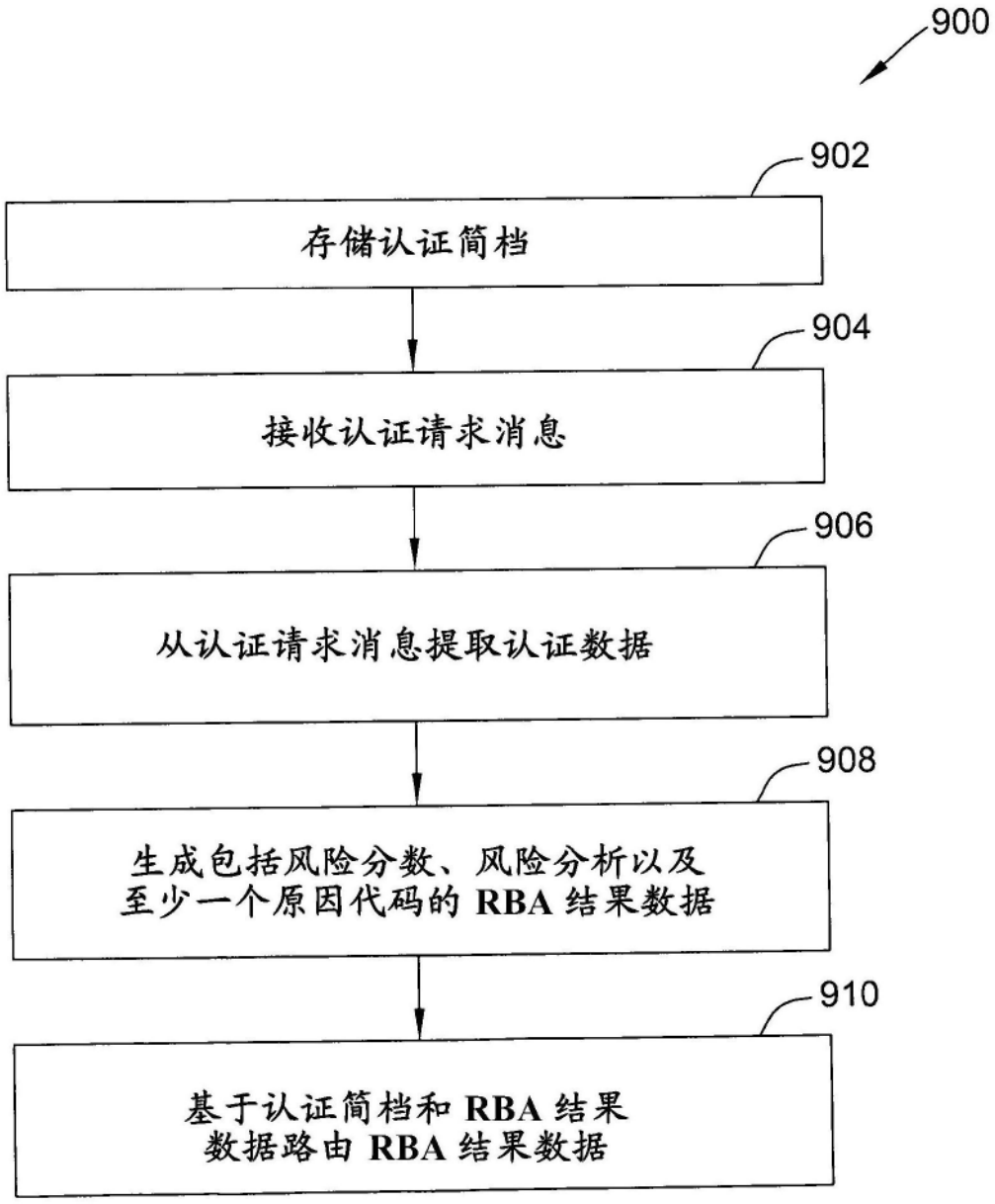

900
902
存储认证简档
904
接收认证请求消息
906
从认证请求消息提取认证数据
908
生成包括风险分数、风险分析以及
至少一个原因代码的 RBA 结果数据
910
基于认证简档和 RBA 结果
数据路由 RBA 结果数据

图9

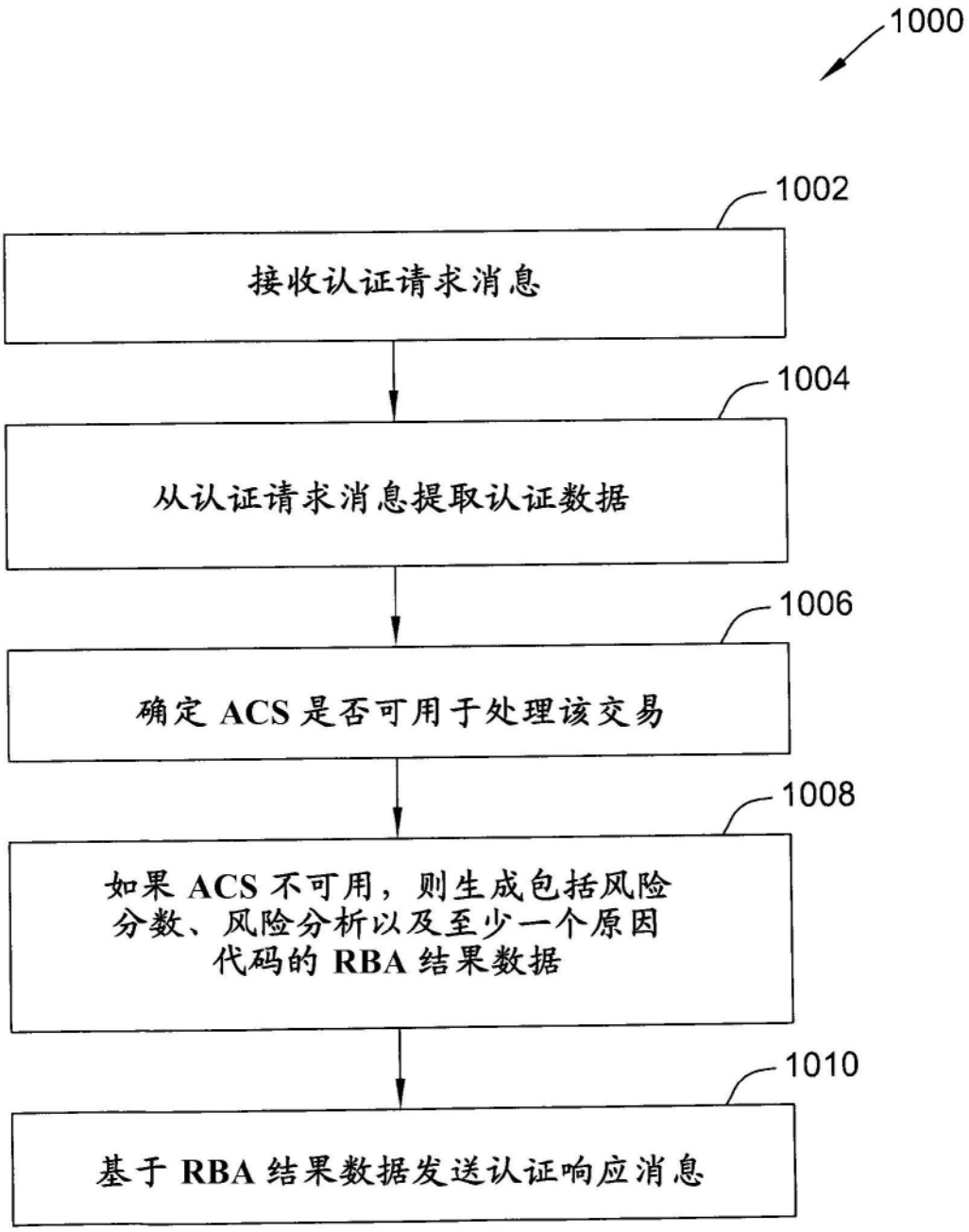

1000
1002
接收认证请求消息
1004
从认证请求消息提取认证数据
1006
确定 ACS 是否可用于处理该交易
1008
如果 ACS 不可用，则生成包括风险分数、风险分析以及至少一个原因代码的 RBA 结果数据
1010
基于 RBA 结果数据发送认证响应消息

图10

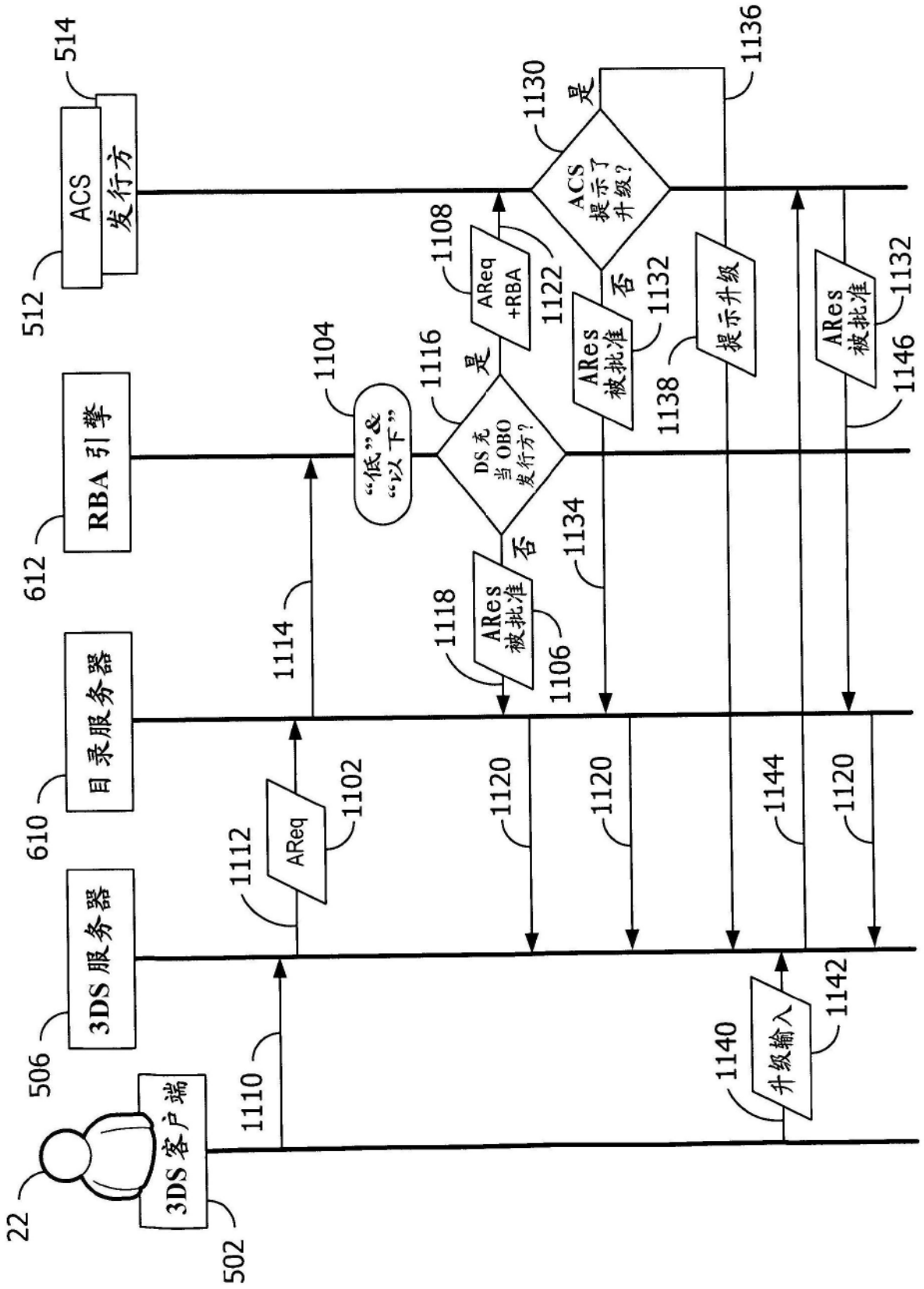

22
3DS 客户端
502
3DS 服务器
506
目录服务器
610
RBA 引擎
612
ACS
发行方
512
514
1110
AReq
1112
1102
1114
“低”&
“以下”
1104
DS 无
当 OBO
发行方?
1116
是
否
AReq
+RBA
1108
1122
ACS
提示了
升级?
1130
是
否
1132
1134
ARes
被批准
1118
1106
1120
1120
1120
1136
提示升级
1138
1144
ARes
被批准
1146
1132
升级输入
1140
1142

图11A

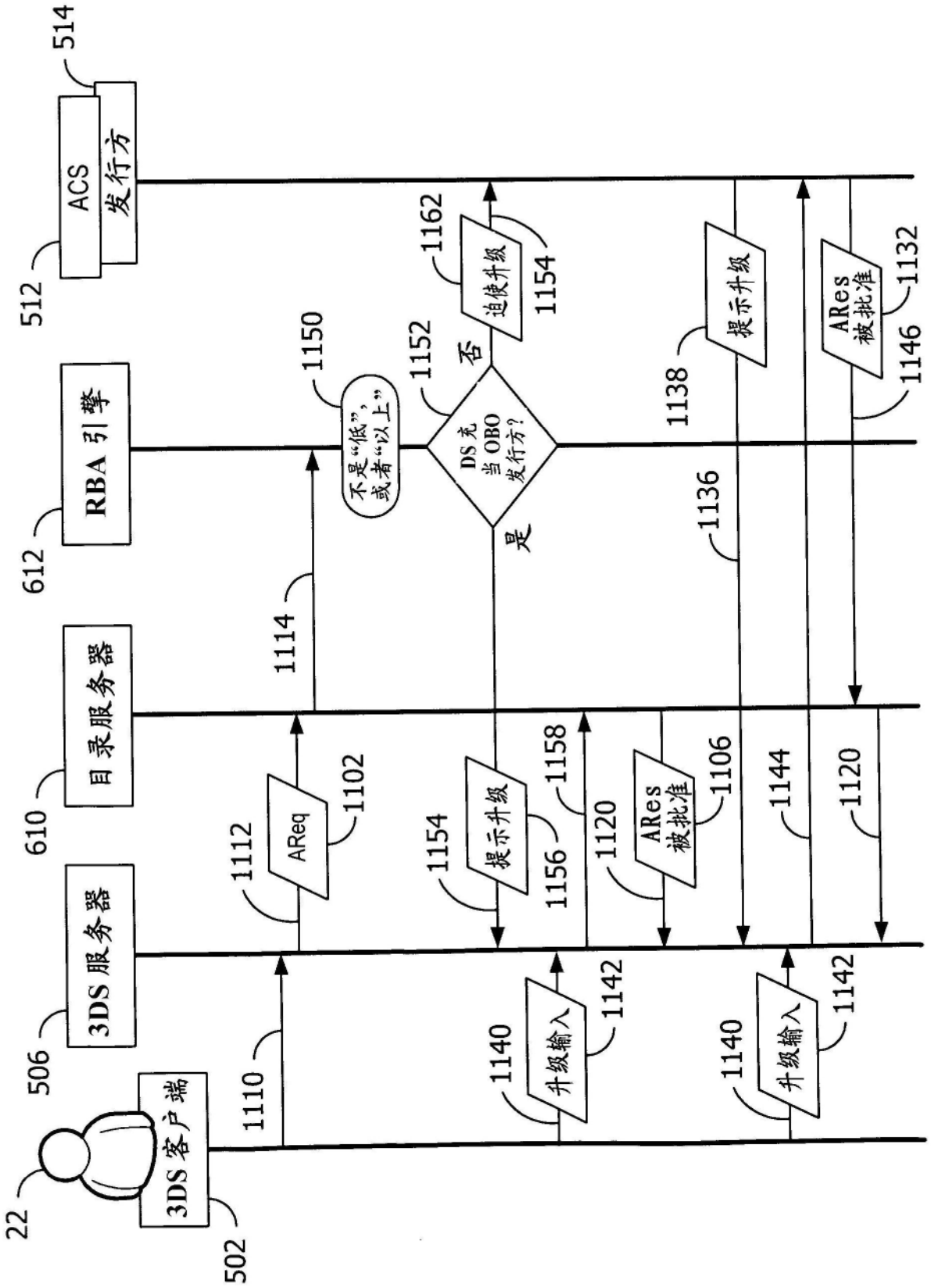

22
3DS 客户端
502
3DS 服务器
506
目录服务器
610
RBA 引擎
612
ACS
发行方
512
514
1110
1112
AReq
1102
1114
不是“低”，或者“以上”
1150
DS 充当 OBO 发行方?
1152
否
是
1154
迫使升级
1162
1154
提示升级
1156
1158
1120
ARes 被批准
1106
1136
1138
提示升级
1144
1120
ARes 被批准
1146
1132
1140
升级输入
1142
1140
升级输入
1142

图11B

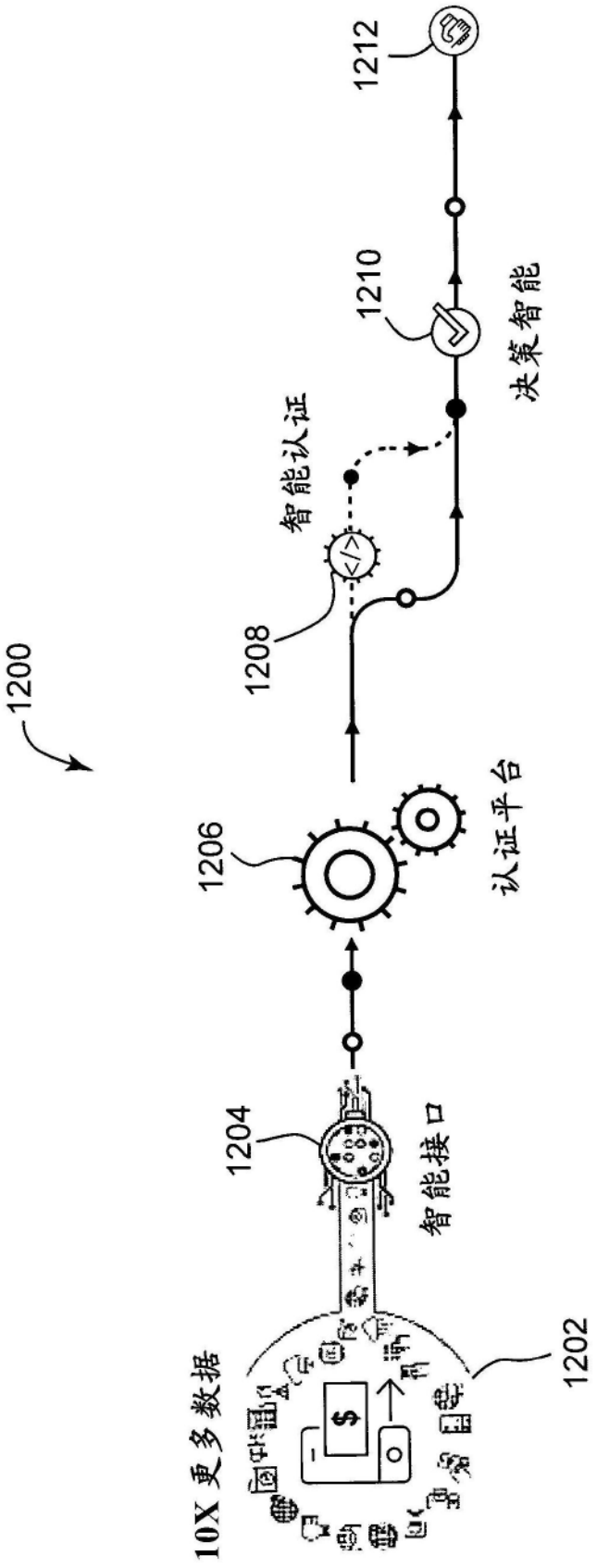

1200
1202
10X 更多数据
1204
智能接口
1206
认证平台
1208
智能认证
1210
决策智能
1212

图12