(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 107710257 B
(45)授权公告日 2021.08.24

(21)申请号 201680032021.9
(22)申请日 2016.04.13
(65)同一申请的已公布的文献号
申请公布号 CN 107710257 A
(43)申请公布日 2018.02.16
(30)优先权数据
1507047.7 2015.04.24 GB
(85)PCT国际申请进入国家阶段日
2017.12.01
(86)PCT国际申请的申请数据
PCT/GB2016/051033 2016.04.13
(87)PCT国际申请的公布数据
WO2016/170305 EN 2016.10.27
(73)专利权人 VISA欧洲有限公司
地址 英国伦敦
(72)发明人 布赖恩·沙利文 戴维·威尔逊 戴维·哈尔比格
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 田喜庆
(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
(56)对比文件
US 2003061171 A1,2003.03.27
US 2011161233 A1,2011.06.30
CN 105408927 A,2016.03.16
审查员 马驰

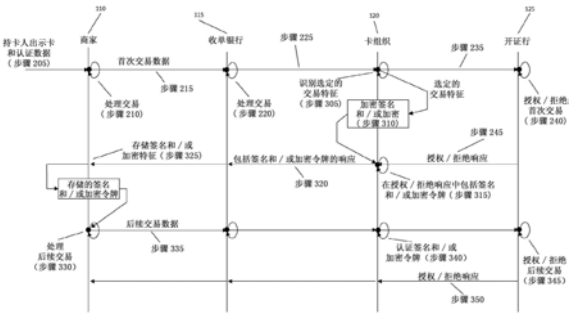
权利要求书2页 说明书5页 附图3页

(54)发明名称

保留交易上下文的方法

(57)摘要

提供了一种交易认证的方法。在一个这种方法中,已经进行了至少一个第一交易,该第一交易或每个第一交易生成包含第一数据和第二数据的数据,第一数据包括认证数据,第二数据标识该第一交易或每个第一交易,其中,给定的第一交易是在商家与持卡人之间。在该方法中,至少使用所第二数据生成对应于给定的第一交易、且包括第一交易的特征的密码签名和/或加密令牌。对应于给定的第一交易的密码签名和/或加密令牌被发送至商家。该方法包括:从商家接收对应于第二交易的数据;并且在对应于第二交易的数据包括密码签名和/或加密令牌的情况下,响应地认证密码签名和/或加密令牌,从而确定第二交易与给定的第一交易之间的经认证的关联。



CN 107710257 B

1.一种交易认证方法,其中,卡组织的计算机系统:

接收与商家和卡持有者之间的第一交易相对应的数据,与所述第一交易相对应的数据包括:包含认证数据的第一数据和识别所述第一交易的第二数据;

通过对至少所述第一数据和所述第二数据进行密码签名和/或加密,生成对应于所述第一交易的令牌;

将对应于所述第一交易的令牌发送给所述商家;

从所述商家接收对应于第二交易的数据;并且

在对应于所述第二交易的所述数据包括对应于所述第一交易的令牌的情况下,响应地验证所述令牌,从而基于所述第一交易的认证来认证所述第二交易。

2.根据权利要求1所述的方法,进一步包括将指示所述令牌的验证的结果的数据发送至支付卡发行者。

3.根据权利要求1所述的方法,进一步包括将指示所确定的所述第二交易的认证的数据发送至支付卡发行者。

4.根据权利要求2所述的方法,其中,所述第二交易包括所述第一交易的重新提交。

5.根据前述权利要求中任一项所述的方法,其中,所述第一交易是EMV交易并且其中所述第一数据包括EMV认证数据。

6.根据权利要求1所述的方法,其中,所述第一交易是无卡交易并且其中所述第一数据包括卡和/或持卡人认证数据。

7.根据权利要求6所述的方法,其中,所述卡和/或持卡人认证数据包括卡安全码、CSC、认证数据之一。

8.根据权利要求1所述的方法,其中,至少所述第二交易是一系列经常性交易中的一个,所述一系列经常性交易中的每一个根据预定计划表发生。

9.根据权利要求1所述的方法,其中,所述第一交易包括用于包括至少所述第二交易的一个或多个后续交易的授权,并且其中,当执行所述第一交易时,所述一个或多个后续交易的数量、时刻和货币金额中的至少一个是未知的。

10.一种非临时性计算机可读存储介质,包括存储在其上的一组计算机可读指令,在由卡组织的计算机系统的至少一个处理器执行时,使得所述至少一个处理器:

接收与商家和卡持有者之间的第一交易相对应的数据,与所述第一交易相对应的数据包括:包含认证数据的第一数据和识别所述第一交易的第二数据;

通过对至少所述第一数据和所述第二数据进行密码签名和/或加密,生成对应于所述第一交易的令牌;

将对应于所述第一交易的令牌发送给所述商家;

从所述商家接收对应于第二交易的数据;并且

在对应于所述第二交易的所述数据包括对应于所述第一交易的令牌的情况下,响应地验证所述令牌,从而基于所述第一交易的认证来认证所述第二交易。

11.一种用于交易认证的装置,包括:

至少一个处理器;

以及包括计算机程序指令的至少一个存储器;

利用所述至少一个处理器,所述至少一个存储器和所述计算机程序指令被配置为使得

所述装置：

接收与商家和卡持有者之间的第一交易相对应的数据，与所述第一交易相对应的数据包括：包含认证数据的第一数据和识别所述第一交易的第二数据；

通过对至少所述第一数据和所述第二数据进行密码签名和/或加密，生成对应于所述第一交易的令牌；

将对应于所述第一交易的令牌发送给所述商家；

从所述商家接收对应于第二交易的数据；并且

在对应于所述第二交易的所述数据包括所述令牌的情况下，响应地验证所述令牌，从而基于所述第一交易的认证来认证所述第二交易。

保留交易上下文的方法

技术领域

[0001] 本公开涉及用于在使用支付卡进行的交易中保留上下文的方法、系统和计算机程序。

背景技术

[0002] 持卡人与商家之间的交易通常涉及持卡人和/或卡的一定程度的认证。例如,EMV(Europay、MasterCard、Visa)标准提供“芯片和PIN”认证,其中,POS(销售点)读卡器读取支付卡(诸如,信用卡或者借记卡)上的集成电路(芯片),持卡人输入PIN,并且核对由持卡人输入的PIN与例如存储在芯片上的数据的关系。如另一实例,交易可以是无卡交易,例如,不向商家实际地出示支付卡的邮购订单交易。持卡人可以提供包括CSC(卡安全码)的认证数据。这些认证方法以及许多其他方式在本领域中是众所周知的。除了持卡人的认证之外,典型的认证方法可包括卡本身的认证,例如,通过处理使用存储在卡上的秘密数据产生的认证数据。通常包括指示认证的数据的交易数据经由卡组织(card scheme)发送至用于授权的开证行。例如,当由持卡人输入的PIN被存储在卡上的数据成功核对时,交易数据可包括指示认证数据的成功验证的标记。在其他系统中,可以发送由用户输入的PIN用于由例如卡组织或开证行的认证。当决定是否拒绝或授权交易时,由开证行考虑认证的结果。认证数据还可以由卡组织核对。为了安全原因,通常情况下不允许商家存储认证数据。

[0003] 商家可以提交与先前交易相关联的一个或多个交易。例如,如果在先前交易时商家与例如卡组织或开证行之间的连接是不可能的,则可能延迟这个交易的提交直到持卡人已经拥有与该交易相关的货物和/或服务之后。如果先前交易当时被拒绝,例如,由于持卡人的账号中的资金不足,则商家可能希望随后重新提交这个交易,期待自此已经补充资金。在另一实例中,持卡人可能希望安排一系列经常性交易,例如,按月支付。在这些实例的两个实例中,已经认证了至少一个先前交易,但是因为不允许商家存储交易认证数据,因此用于先前交易的认证数据在随后的交易或一些交易时是不可用的。

[0004] 允许与先前交易相关联的后续交易的提交的已知系统在没有完整认证数据的情况下有效地允许交易。这存在安全风险,因为这种交易更容易被骗。因此,一些卡提供者不允许交易重新提交或者经常性交易。

[0005] 因此,需要一种用于对与先前交易相关联的交易进行认证的安全方法,而不要求卡提供者维护大型交易数据库。

发明内容

[0006] 根据本公开的第一方面,提供了交易认证的方法,其中:已经进行了至少一个第一交易,该第一交易或每个第一交易产生包括包含认证数据的第一数据以及标识该第一交易或每个第一交易的第二数据,其中,给定的第一交易是在商家与持卡人之间;其中,至少使用所述第二数据产生对应于给定的第一交易并包括第一交易的特征的密码签名和/或加密令牌;并且其中,对应于给定的第一交易的密码签名和/或加密令牌被发送至商家,该方法

包括：

[0007] 从商家接收对应于第二交易的数据;并且

[0008] 在对应于第二交易的数据包括密码签名和/或加密令牌的情况下,响应地认证密码签名和/或加密令牌,从而确定第二交易与给定的第一交易之间的经认证的关联。

[0009] 因此,基于认证的第一交易为第二交易的认证提供了有效且安全的方法,而无需独立地生成认证数据。应注意,如本文中使用的术语“认证数据”包含指示通过例如读卡器的认证是成功的一个标记或多个标记、由用户输入的PIN、CSC卡标识符以及将由技术人员容易理解的其他合适形式的认证。认证的这种其他形式的实例包括生物特征认证、3DSecure、以及持卡人登录详情的认证。该认证可以是对持卡人的身份的认证、卡的认证、或者这两者的认证。

[0010] 该方法可以进一步包括将表示密码签名和/或加密令牌的所述认证的结果的数据发送至支付卡发行者。在一个实施方式中,该方法包括将指示所确定的经认证的关联的数据发送至支付卡发行者。因此,发行者可以确信第二交易与第一交易相关联。例如,发行者可以在决定接受或拒绝第二交易时使用这个结果。

[0011] 在又一实施方式中,第二交易包括第一交易的重新提交。因此商家无需存储除了第一交易的令牌和标识符之外的任何认证数据,日后就可以重新提交失败的交易,例如,希望持卡人已经向他们的账号补充资金;因此利用第一交易安全地识别了重新提交。

[0012] 根据一些安排,第一交易是EMV交易并且第一数据包括EMV认证数据。因此,商家使用建立的且可信的EMV协议(需要在销售点出示支付卡)的第一交易可以可信地与第二交易相关联(不用为此提供EMV认证数据)而无需存储除了令牌之外的认证数据。

[0013] 在一些其他安排中,第一交易是无卡交易并且其中第一数据包括卡和/或持卡人认证数据。卡和/或持卡人认证数据可以包括卡安全码、CSC、认证数据。因此,商家使用建立的CSC协议的第一交易可以可信地与第二交易相关联(不用为此提供CSC认证数据)而无需存储除了令牌之外的认证数据。

[0014] 根据本公开的一些方面,至少第二交易是一系列经常性交易中的一个,并且一系列经常性交易中的每一个根据预定计划表发生。像这样的,没有为此提供认证数据的经常性交易的这种计划表可以安全地与为此提供认证数据的第一交易相关联。具体地,允许商家提交经常性交易而无需存储除了第一交易的令牌和标识符之外的任何认证数据;因此存在利用第一交易安全识别重新提交的信心。

[0015] 根据本公开的又一方面,第一交易包括用于一个或多个后续交易(包括至少第二交易)的授权,并且其中,当执行第一交易时,一个或多个后续交易的数量、时刻和货币金额中的至少一个是未定的。这允许不用为此提供认证数据的这种后续交易与第一交易相关联,该第一交易授权后续交易并且为此提供认证数据。

[0016] 本发明的进一步特征和优点将参考附图从仅通过实例的方式给定的本发明的优选实施方式的以下描述中变得显而易见。

附图说明

[0017] 图1示出了在其内本公开的实施方式可以实施的系统架构。

[0018] 图2示出了用于处理认证数据可用的首次交易以及认没有证数据可用的后续交易

的方法。

[0019] 图3示出了用于处理首次交易和后续交易的方法,使用对应于第一交易的密码签名和/或加密令牌来确定两个交易之间的经认证的关联。

具体实施方式

[0020] 图1中示出了根据本公开的实施方式的系统架构,其描述了根据用于卡支付的已知的四方模式配置的系统。持卡人105与商家110进行交易。商家可以与收单银行115通信。收单银行可与卡组织120通信,该卡组织依次可以与开证行125通信。

[0021] 图2示出了这种系统中的传统示例性交易。持卡人105向商家110出示卡和认证数据(步骤205)。认证数据可以是例如由持卡人提供的PIN或者签名。如另一实例,如果交易是无卡交易,则认证数据可以是CSC。其他形式的认证在本领域中是已知的。

[0022] 商家处理该交易(步骤210),例如,该步骤可包括捕获关于该交易的详情,并且验证由持卡人提供的认证数据。这种处理产生交易数据。如果该交易在销售点被验证,例如通过卡上的处理器验证认证数据,则该交易数据通常包括该验证的结果的指示,例如,指示持卡人正确输入PIN的标记。可替换地,如果在销售点未验证认证数据,则认证数据可以被包括在交易数据中以供例如卡组织120或者开证行125进行后续验证。在商家验证认证数据的一些实施方式中,如果验证失败,则商家根本不发送任何交易数据。

[0023] 商家110将交易数据发送至收单银行115(步骤215),该收单银行可以执行例如验证交易的详情的额外处理(步骤220)。收单银行115将交易数据发送至卡组织120(步骤225)。卡组织120可以处理交易数据(步骤230),例如执行额外的认证。然后卡组织120将交易数据发送至开证行125。开证行125处理交易数据,包括决定是否授权或拒绝该交易(步骤240)。这个决定结果至少部分基于认证数据;例如,如果认证方法是相对安全的,诸如,EMV“芯片和PIN”认证,则开证行125更可能接受该交易,并且如果认证方法较不安全,诸如,无卡交易中的CSC认证,则不太可能接受该交易。开证行125将该决定结果发送至卡组织120(步骤245),该决定结果从卡组织被发送至收单银行115并且由此发送至商家110。

[0024] 如上所述,商家110可以提交与上述首次交易相关联的一个或多个后续交易。商家110处理这种后续交易(步骤250),产生交易数据。如上所述,不允许商家存储首次交易的认证数据。进一步的认证数据在后续交易时不可用,例如,在没有持卡人输入的情况下触发后续交易时。因而,认证数据往往不适用于第二次交易。如同首次交易一样,商家110将后续交易的交易数据发送至收单银行115,该交易数据从收单银行115发送至卡组织120。卡组织120将交易数据发送至开证行125。关于首次交易,开证行125处理包括决定是否授权或者拒绝后续交易的交易数据(步骤260)。因为认证数据不适用于后续交易,所以开证行通常不太可能授权该交易,因为它对交易是合法的具有较小确定性。这个决定结果然后经由卡组织120和收单银行115从开证行125发送至商家110(步骤265)。

[0025] 现在将参考图3描述根据本公开实施方式的改善方法的描述。如上所述,持卡人105向商家110出示卡和认证数据(步骤205),以执行首次交易。

[0026] 商家处理首次交易(步骤210),其可以包括例如捕获与交易有关的详情。这种处理产生交易数据,该交易数据包括例如由持卡人提供的认证数据或者表示在销售点处验证认证数据的结果的数据。

[0027] 商家110将交易数据发送至收单银行115(步骤215)，该收单银行可以执行额外处理，例如验证交易的详情(步骤220)。收单银行115将交易数据发送至卡组织120(步骤225)。卡组织120处理交易数据并且识别该交易的选定特征(步骤305)。选定特征可包括例如唯一的交易标识符、交易的日期和/或时间、标识商家110的数据、标识收单银行115的数据、标识商家110的数据、以及标识认证上下文的数据，例如标识使用了EMV“芯片和PIN”认证。卡组织120对选定的一个或多个交易特征进行密码签名和/或加密(步骤310)，生成对应于首次交易且包含第一交易的特征的密码签名和/或加密令牌(此后简单地称为“令牌”)。该令牌还可以包括其他数据。例如，这样的其他数据可以描述约束，诸如，有限的有效期、可以与首次交易有效地相关联的后续交易的类型的限制、或者允许这种后续交易通过的通道。如以下将说明的，这个令牌可以随后由卡组织120来验证，并且可以使用私钥密码技术。合适的私钥密码处理的实例是DES、Triple DES、AES、Twofish、Serpent、Blowfish、CAST5、RC4、Skipjack和IDEA。可替换地，可以使用公钥密码技术。这种公钥密码处理的实例包括RSA和椭圆曲线密码学。使用公钥密码的优点在于可以通过拥有相关公钥证书的任何实体验证该令牌。

[0028] 卡组织120将交易数据发送至处理交易数据的开证行125(步骤235)以特别决定是否授权或者拒绝该交易(步骤240)。开证行125然后将该决定结果发送至卡组织120(步骤245)。

[0029] 在本公开的一些方面，卡组织120包括在表示授权或者拒绝该交易的决定结果的消息中包括令牌(步骤315)。这个结合消息然后被发送至收单银行115(步骤320)，该收单银行将该消息转发至商家110。可替换地，卡组织120可以将该令牌与授权或者拒绝该交易的决定结果分开发送至商家110。

[0030] 商家110然后存储该令牌(步骤325)，这意味着如果商家110提交与第一交易相关联的后续交易的情况下，如步骤330和335中所示，则可以与对应于后续交易的其他交易详情一起发送该令牌。应注意，这与关于诸如首次交易的任何特定交易的认证数据(其不可以被商家存储)的情况不同，因为可以允许商家存储令牌。

[0031] 卡组织120然后尝试认证该令牌(步骤340)，从而确定首次交易与后续交易之间的经认证的关联。由于令牌是使用来自首次交易的完整认证数据生成的，因此对令牌的成功验证授予了首次交易真实发生并被成功认证的信任度。因此，令牌的认证提供了后续交易合法性的信任度，因此开证行更可能批准后续交易。在可替换的实施方式中，可以通过除了卡组织之外的实体(例如，开证行)来认证该令牌。

[0032] 卡组织120然后可将表示令牌的认证的数据、或者表示令牌的认证结果的数据发送至开证行125。开证行125可以在决定是否授权或者拒绝后续交易时(步骤345)使用这些数据。令牌的成功认证提供了第一交易与后续交易之间的经认证的关联，因此与没有完整认证数据的后续交易(诸如，图2中描述的)相比，开证行更可能授权这种后续交易。

[0033] 开证行125将授权或拒绝后续交易的决定结果发送至卡组织120(步骤350)。该结果然后从卡组织120转发至收单银行115，并且从收单银行115转发至商家110。

[0034] 以上描述的方法基于认证的首次交易为后续交易的认证提供了有效且安全的方法，而不要求单独的认证数据。

[0035] 后续交易例如可以是在拒绝首次交易之后的首次交易的重新提交。可替换地，可

以是一系列经常性交易中的一个，每一个经常性交易根据预定计划表进行。描述这个计划表的信息可以被包括在该令牌中。如另一实例，首次交易和后续交易可以包括分拆交易，其中，大交易被分成较小的交易并且分开计费。

[0036] 应注意，本公开中使用单词“步骤”不意味着以任何特定顺序执行这些步骤。作为说明性实例，参考图3，可以在步骤310之前、之后或者并行执行步骤235。

[0037] 还应注意，术语“商家”、“收单银行”、“卡组织”和“开证行”被理解为指被配置为执行以上所描述的功能的计算机化系统。

[0038] 以上所描述的示例性实施方式可以以许多方式(诸如用于由处理器执行的程序指令)来实现为逻辑电路、专用集成电路、固件等。例如，本实施方式可被实现为一个或多个软件或者固件应用程序、计算机实现的方法、存储在计算机可用介质上的用于在一个或多个处理器(例如，CPU、微控制器)或无线基站中的其他计算设备上执行的程序产品。

[0039] 上述实施方式应被理解为本发明的说明性实例。设想了又一实施方式。例如，当持卡人使用服务或者购买产品(例如，出租车服务或者在酒吧开单)时，可以基于单个首次交易进行多个不规则的间隔的后续交易。因此首次交易可以包含用于后续交易的预授权。在又一实施方式中，本公开允许扩大授权，例如，如果持卡人决定延长其在酒店的停留时间。如另一实例，首次交易可以包含预订例如宾馆或者旅行社，并且后续交易可以涉及随后升级或附加服务、或者不显示费用、或者诸如使用迷你酒吧的辅助性费用。例如，这将允许持卡人在宾馆入住之后适当交费而不必实际在结账中出现。本公开的又一实施方式将允许分期付款。如另一实例，本公开允许债务追收交易，例如，用于可变票价公共交通。在这种实施方式中，可以在持卡人使用了交通服务之后尝试交易，例如，在一天的结束的时候。如果在一天中进行了多个旅程，则例如可允许降低票价。如果该交易被拒绝，例如，由于持卡人的账号中资金不足，则可以尝试根据本公开的后续交易以收回该债务。

[0040] 应理解的是，关于任何一个实施方式描述的任何特征可以单独地或者与所描述的其他特征相结合地使用，并且还可以与任何其他实施方式的一个或多个特征或者与任何其他实施方式的任何组合相结合地使用。此外，在不背离在所附权利要求中限定的本发明的范围的情况下，可采用以上没有描述的等同物和修改。

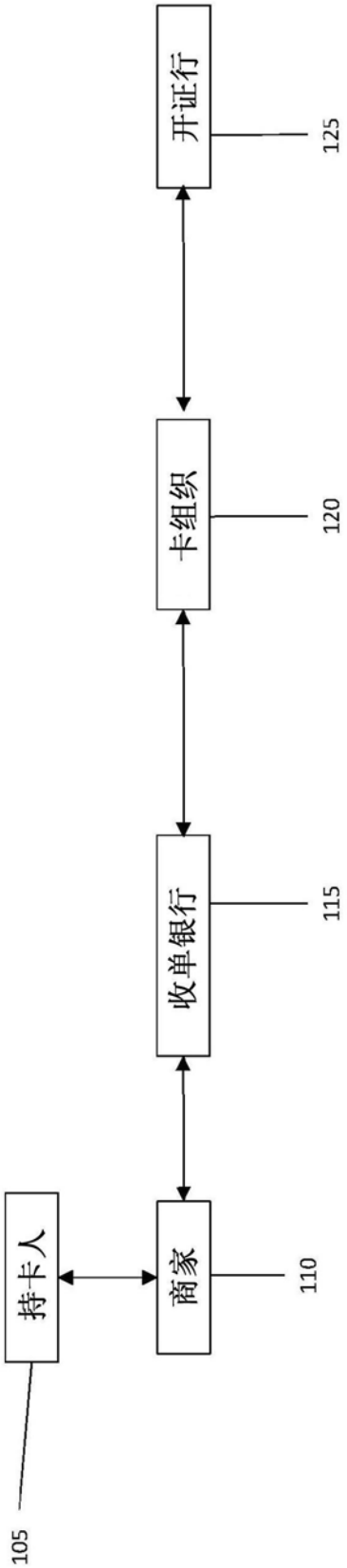


图1

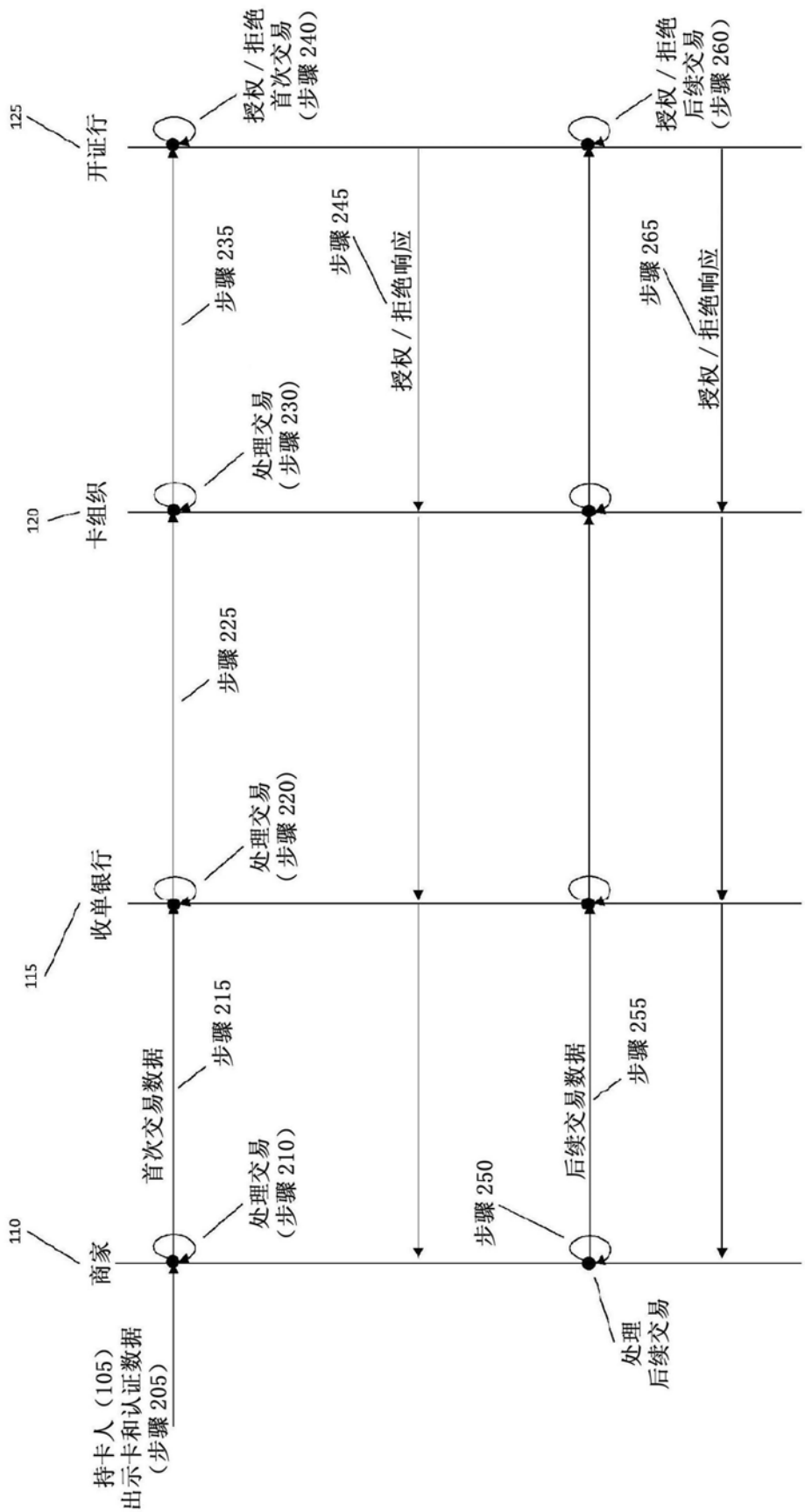

持卡人（105）
出示卡和认证数据
（步骤205）
110
商家
处理交易
（步骤210）
首次交易数据
步骤215
115
收单银行
处理交易
（步骤220）
步骤225
120
卡组织
处理交易
（步骤230）
步骤235
125
开证行
授权／拒绝
首次交易
（步骤240）
步骤245
授权／拒绝响应
步骤250
处理
后续交易
后续交易数据
步骤255
步骤265
授权／拒绝响应
授权／拒绝
后续交易
（步骤260）

图2

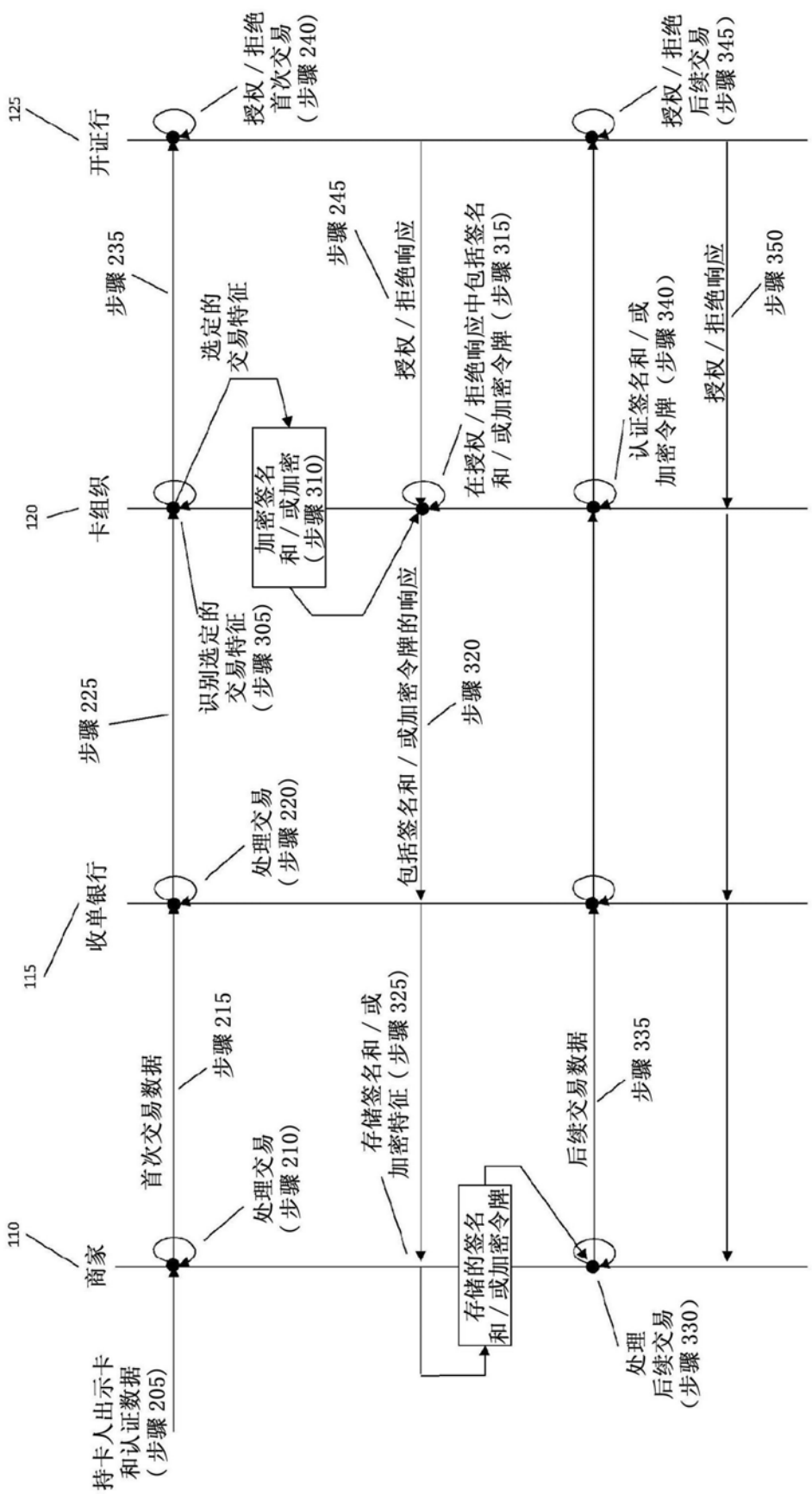

110
商家
115
收单银行
120
卡组织
125
开证行
持卡人出示卡和认证数据（步骤205）
处理交易（步骤210）
步骤215
首次交易数据
处理交易（步骤220）
步骤225
识别选定的交易特征（步骤305）
选定的交易特征
步骤235
加密签名和/或加密（步骤310）
授权/拒绝首次交易（步骤240）
步骤245
授权/拒绝响应
包括签名和/或加密令牌的响应
步骤320
存储签名和/或加密特征（步骤325）
存储的签名和/或加密令牌
在授权/拒绝响应中包括签名和/或加密令牌（步骤315）
后续交易数据
步骤335
处理后续交易（步骤330）
认证签名和/或加密令牌（步骤340）
授权/拒绝后续交易（步骤345）
授权/拒绝响应
步骤350

图3