(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114788223 A
(43)申请公布日 2022.07.22

(21)申请号 202080085543.1
(22)申请日 2020.12.11
(30)优先权数据
62/947,712 2019.12.13 US
(85)PCT国际申请进入国家阶段日
2022.06.09
(86)PCT国际申请的申请数据
PCT/US2020/064616 2020.12.11
(87)PCT国际申请的公布数据
WO2021/119495 EN 2021.06.17
(71)申请人 维萨国际服务协会
地址 美国加利福尼亚州
(72)发明人 R·莱瓦 P·罗伊
(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 徐倩 周全
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
G06Q 20/38(2012.01)

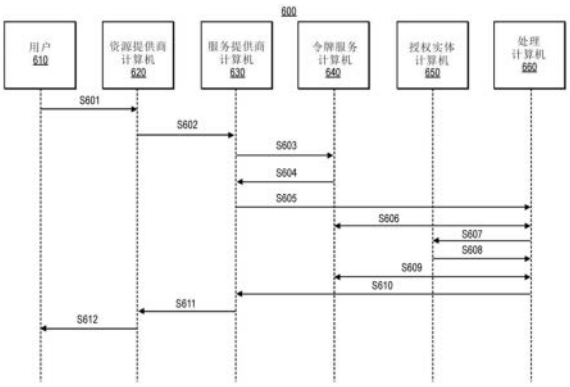
权利要求书2页 说明书13页 附图9页

(54)发明名称

令牌管理系统和方法

(57)摘要

公开了一种方法。所述方法包括向令牌服务计算机发送包括与所述令牌请求方相关联的令牌请求方标识符和与所述服务提供商计算机相关联的服务提供商计算机标识符的请求消息。所述方法还包括接收包括令牌和/或密码的响应消息,生成包括所述令牌和所述密码的授权请求消息,以及向与令牌服务计算机通信的处理计算机发送所述授权请求消息。



CN 114788223 A

1.一种方法,包括:

由服务提供商计算机从令牌请求方计算机接收交易发起消息;

由所述服务提供商计算机向令牌服务计算机发送包括与所述令牌请求方相关联的令牌请求方标识符和与所述服务提供商计算机相关联的服务提供商计算机标识符的请求消息;

响应于发送密码请求消息,由所述服务提供商计算机接收包括令牌和/或密码的响应消息;

由所述服务提供商计算机生成包括所述令牌和所述密码的授权请求消息;

由所述服务提供商计算机将所述授权请求消息发送到与令牌服务计算机通信的处理计算机,其中所述处理计算机结合所述令牌服务计算机来确定与所述令牌相关联的真实凭证并验证所述密码;以及

响应于发送所述授权请求消息,由所述服务提供商计算机从所述处理计算机接收授权响应消息。

2.根据权利要求1所述的方法,其中所述密码是仅在特定交互信道中有效的信道特定密码。

3.根据权利要求1所述的方法,其中所述请求消息是进一步包括所述令牌或令牌标识符的密码请求消息,并且其中所述令牌服务计算机在生成所述密码之前验证所述令牌、与所述令牌请求方相关联的所述令牌请求方标识符和所述服务提供商计算机标识符彼此相关联。

4.根据权利要求3所述的方法,其中所述令牌服务计算机包括将所述服务提供商标识符与所述令牌请求方标识符映射的表。

5.根据权利要求3所述的方法,其中由所述服务提供商计算机向所述令牌服务计算机发送包括所述令牌或令牌标识符、与所述令牌请求方相关联的所述令牌请求方标识符和与所述服务提供商计算机相关联的所述服务提供商计算机标识符的所述密码请求消息包括:由所述服务提供商计算机向所述令牌服务计算机发送包括所述令牌标识符、与所述令牌请求方相关联的所述令牌请求方标识符和与所述服务提供商计算机相关联的所述服务提供商计算机标识符的所述密码请求消息。

6.根据权利要求1所述的方法,其中所述令牌请求方是资源提供商计算机。

7.根据权利要求1所述的方法,其中所述令牌是以数学方式从所述真实凭证生成的。

8.根据权利要求1所述的方法,其中所述令牌请求方计算机从与用户相关联的用户装置接收交互请求。

9.根据权利要求1所述的方法,其中所述请求消息用在所述令牌服务计算机与所述服务提供商计算机之间共享的第一密码密钥对中的密码密钥加密,其中所述第一密码密钥对不同于在所述令牌请求方计算机与所述服务提供商计算机之间共享的第二密码密钥对。

10.一种服务提供商计算机,包括:

处理器;以及

包括指令的非瞬态计算机可读介质,所述指令在由所述处理器执行时使得所述处理器:

从令牌请求方计算机接收交易发起消息;

向令牌服务计算机发送包括与所述令牌请求方相关联的令牌请求方标识符和与所述服务提供商计算机相关联的服务提供商计算机标识符的请求消息；

响应于发送密码请求消息，接收包括令牌和/或密码的响应消息；

生成包括所述令牌和所述密码的授权请求消息；

将所述授权请求消息发送到与令牌服务计算机通信的处理计算机，其中所述处理计算机结合所述令牌服务计算机来确定与所述令牌相关联的真实凭证并验证所述密码；以及

响应于发送所述授权请求消息，从所述处理计算机接收授权响应消息。

11.根据权利要求10所述的服务提供商计算机，其中所述请求消息是密码请求消息且包括所述令牌。

12.根据权利要求10所述的服务提供商计算机，其中所述令牌请求方标识符是令牌请求方ID，并且所述服务提供商计算机标识符是令牌请求方-令牌服务提供商ID。

13.根据权利要求10所述的服务提供商计算机，其中所述密码从所述令牌请求方标识符和所述服务提供商计算机标识符形成。

14.根据权利要求10所述的服务提供商计算机，其中所述真实凭证是PAN。

15.一种方法，包括：

由服务提供商计算机向令牌服务计算机发送令牌请求消息，所述令牌请求消息包括与所述服务提供商计算机相关联的服务提供商标识符和与能操作地耦合到所述服务提供商系统的多个令牌请求方中的令牌请求方相关联的令牌请求方标识符；

响应于发送所述令牌请求消息，由所述服务提供商计算机从所述令牌提供商系统接收令牌；以及

由所述服务提供商计算机向所述令牌请求方发送所述令牌。

16.根据权利要求15所述的方法，其中所述令牌提供商系统包括数据库，所述数据库包括将所述服务提供商标识符与所述令牌请求方标识符映射的表。

17.根据权利要求15所述的方法，其中所述令牌请求消息或包含在所述令牌请求消息中的数据使用用于保护所述服务提供商计算机与所述令牌服务计算机之间的通信的第一密码密钥对中的密码密钥加密。

18.根据权利要求17所述的方法，其中所述服务提供商系统和所述令牌请求方使用第二密码密钥对来保护所述服务提供商系统与所述令牌请求方之间的通信，当所述令牌从所述服务提供商计算机发送到所述令牌请求方时，所述令牌用所述第二密码密钥对中的密码密钥加密。

19.根据权利要求15所述的方法，其中所述令牌的长度为16位数字。

20.根据权利要求15所述的方法，其中所述令牌请求消息或所述令牌请求消息中包含的数据使用用于保护所述服务提供商计算机与所述令牌服务计算机之间的通信的第一密码密钥对中的密码密钥加密，并且其中所述服务提供商系统和所述令牌请求方使用第二密码密钥对来保护所述服务提供商系统与所述令牌请求方之间的通信，当所述令牌从所述服务提供商计算机发送到所述令牌请求方时，所述令牌用所述第二密码密钥对中的密码密钥加密，并且其中所述第一密码密钥对和所述第二密码密钥对各自是对称密钥对。

令牌管理系统和方法

[0001] 相关申请交叉引用

[0002] 本申请是PCT申请,其要求2019年12月13日提交的第62/947,712号美国临时申请的优先权,所述美国临时申请以全文引用的方式并入本文中。

背景技术

[0003] 令牌请求方可以使用令牌来处理交易,而不是使用真实凭证来处理交易。然而,在一些情况下,许多令牌请求方可能与单个服务提供商配合以进行交易。令牌请求方通常需要向令牌服务计算机注册以处理其令牌化交易。

[0004] 当前系统有一些问题需要解决。例如,对于每个令牌请求方来说,向令牌服务提供商进行注册是繁杂且困难的。如果令牌请求方希望与服务提供商计算机相关联,则每个令牌请求方都需要向服务提供商计算机和令牌服务计算机两者注册。例如,如果有一百个令牌请求方,则每个令牌请求方需要执行两个单独的注册过程,这使得一百个令牌请求方执行总共两百个注册步骤。

[0005] 另一问题是,经由服务提供商计算机连接到令牌服务计算机的多个令牌请求方必须使用不同的加密密钥对。在令牌请求方与令牌服务计算机之间共享的加密密钥用于保护通信,并向令牌服务计算机认证令牌请求方。如果还希望在令牌请求方与服务提供商计算机之间有加密通信,则需要使用不同的加密密钥集合来保护服务提供商计算机与令牌请求方之间的通信。

[0006] 另一要解决的问题是,令牌服务计算机通常在向令牌请求方提供令牌和/或交易密码之前验证令牌请求方。如果令牌服务计算机独立地评估每个令牌请求方,它可能无法准确地评估所述令牌请求方是否可信。如果可以提供额外数据以在向令牌请求方发出令牌或密码之前评估令牌请求方的可信度,将是可取的。

[0007] 本发明的实施例分别解决了这些问题和其它问题。

发明内容

[0008] 本发明的一个实施例涉及一种方法,包括:由服务提供商计算机从令牌请求方计算机接收交易发起消息;由所述服务提供商计算机向令牌服务计算机发送包括与所述令牌请求方相关联的令牌请求方标识符和与所述服务提供商计算机相关联的服务提供商计算机标识符的请求消息;响应于发送密码请求消息,由所述服务提供商计算机接收包括令牌和/或密码的响应消息;由所述服务提供商计算机生成包括所述令牌和所述密码的授权请求消息;由所述服务提供商计算机将所述授权请求消息发送到与令牌服务计算机通信的处理计算机,其中所述处理计算机结合所述令牌服务计算机来确定与所述令牌相关联的真实凭证并验证所述密码;以及响应于发送所述授权请求消息,由所述服务提供商计算机从所述处理计算机接收授权响应消息。

[0009] 本发明的另一实施例涉及一种服务提供商计算机,包括:处理器;以及包括指令的非瞬态计算机可读介质,所述指令在由所述处理器执行时使得所述处理器:从令牌请求方

计算机接收交易发起消息;向令牌服务计算机发送包括与所述令牌请求方相关联的令牌请求方标识符和与所述服务提供商计算机相关联的服务提供商计算机标识符的请求消息;响应于发送密码请求消息,接收包括令牌和/或密码的响应消息;由所述服务提供商计算机生成包括所述令牌和所述密码的授权请求消息;将所述授权请求消息发送到与令牌服务计算机通信的处理计算机,其中所述处理计算机结合所述令牌服务计算机来确定与所述令牌相关联的真实凭证并验证所述密码;以及响应于发送所述授权请求消息,从所述处理计算机接收授权响应消息。

[0010] 本发明的另一实施例包括一种方法,包括:由服务提供商计算机向令牌服务计算机发送令牌请求消息,所述令牌请求消息包括与所述服务提供商计算机相关联的服务提供商标识符和与能操作地耦合到所述服务提供商系统的多个令牌请求方中的令牌请求方相关联的令牌请求方标识符;响应于发送所述令牌请求消息,由所述服务提供商计算机从所述令牌提供商系统接收令牌;以及由所述服务提供商计算机向所述令牌请求方发送所述令牌。

[0011] 下文进一步详细描述本发明的这些和其它实施例。

附图说明

[0012] 图1示出了包括令牌请求方、服务提供商计算机和令牌服务计算机的系统的图式。

[0013] 图2示出了服务提供商计算机使用令牌服务计算机向授权实体计算机注册令牌的系统和过程流程的图式。

[0014] 图3示出了包括令牌请求方、服务提供商计算机和令牌服务计算机的系统的图式。示出了加密密钥对。

[0015] 图4示出了说明用于为资源提供商计算机预配令牌的过程流程的流程图。

[0016] 图5示出了用于为令牌请求方预配用于用户发起的交易和资源提供商发起的交易的令牌的流程图。

[0017] 图6示出了与将现有令牌存档的资源提供商计算机的用户发起的交易的流程图。

[0018] 图7示出了示出资源提供商发起的交易的过程流程的泳道图。

[0019] 图8示出了根据本发明的实施例的服务提供商计算机的框图。

[0020] 图9示出了根据本发明的实施例的令牌服务计算机的框图。

具体实施方式

[0021] 本发明的实施例包括用于由令牌服务计算机向由令牌请求方操作的多个令牌请求方计算机提供唯一令牌请求方标识符(TRID)的系统和方法。令牌请求方与服务提供商计算机相关联。令牌请求方计算机可以经由服务提供商计算机从令牌服务计算机请求令牌。令牌请求方计算机还可以将这些令牌提供给服务提供商计算机以使用所述令牌来处理交易。

[0022] 服务提供商计算机可以使用令牌服务计算机来生成和存储令牌。令牌服务计算机还可以向与令牌请求方通信的服务提供商计算机预配分配给令牌请求方的令牌。令牌服务计算机还可以将令牌、与令牌相关联的真实凭证、令牌请求方标识符(TRID)和服务提供商标识符一起存储在数据库中的令牌请求方记录中。数据库可以为许多不同的令牌请求方存

储许多此类记录。服务提供商计算机可以随后使用令牌服务计算机来处理与所发出令牌的交易。

[0023] 在一些实施例中，服务提供商计算机(例如，数字钱包计算机、社交网络计算机、交易聚合器计算机等)可以向多个令牌请求方提供交易服务，所述多个令牌请求方中的每一个分配有一个或多个令牌。在一些实施例中，令牌请求方可以是商家，并且商家可以使用来自所述商家的多个用户(例如，客户)的令牌。

[0024] 可以将一个或多个唯一标识符分配给每个令牌请求方。例如，令牌请求方可以分配有令牌请求方标识符(TRID)和服务提供商标识符。令牌请求方标识符可以标识令牌请求方，而服务提供商标识符可以标识服务提供商计算机。

[0025] 可以在现有和更改后消息(例如ISO 8583型消息)中发送令牌请求方标识符和服务提供商标识符。例如，十一位数字的令牌请求方标识符(TRID)可以存储在0100TAR/WS API消息的现有标签中，作为<F123 DSID 68.03:XXXXXXXXXXX>，其中X值代表被分配为TRID的唯一值。还可以将标签添加到服务提供商标识符(例如令牌请求方-令牌服务提供商(TR-TSP)标识符)的现有0100TAR/WS API消息，作为<F123 DSID 68.XX:(TR-TSP)标识符>。这些标签也可以存在于通知消息中，例如0600/0620通知消息。

[0026] 另外，令牌服务计算机可以为服务提供商计算机提供单个加密密钥，所述加密密钥可以用于加密在服务提供商计算机与令牌服务计算机之间传递的所有消息，而不考虑与所述消息相关联的令牌请求方计算机。可以通过针对每个令牌请求方计算机-服务提供商计算机关系特别分配的其它密码密钥对来保护在服务提供商计算机与令牌请求方计算机之间传递的消息。

[0027] 令牌请求方计算机的注册可能需要令牌请求方计算机与令牌服务计算机共享某些数据元素。例如，令牌请求方计算机可能需要提供外部客户端ID(例如，由与向令牌服务计算机标识令牌请求方的令牌请求方计算机相关联的服务提供商计算机提供的ID)，令牌请求方标识符(TRID)(例如，由令牌服务计算机分配的令牌请求方ID，如果可用的话)，与令牌请求方相关联的名称(例如，商品名称、法定名称等)，应用程序URL(例如，令牌请求方计算机的应用程序网站URL)，令牌请求方操作所在的国家的国家代码(例如，ISO国家代码)，DUN ID(例如，由Dun和Bradstreet分配的ID)，收单方分配的商家ID(例如，由与商家相关联的收单方分配的用以向收单方标识商家的ID)，和/或政府ID(例如，税务ID)。

[0028] 本发明的实施例具有数个优点。例如，在本发明的实施例中，每个令牌请求方可以使用令牌请求方标识符和服务提供商标识符来从令牌服务计算机请求令牌或密码。因此，令牌服务计算机可以更好地评估是否应该向令牌请求方提供所请求的令牌和/或密码。例如，令牌服务计算机可以评估令牌请求方标识符，以确定其是否有任何可能指示令牌请求方可能是欺诈性的记录。令牌服务计算机还可以评估服务提供商标识符，并且可以确定服务提供商标识符与可信实体相关联。例如，服务提供商可以是具有高安全性标准的数字钱包，并且令牌请求方与可信服务提供商的隶属关系可以进一步证明令牌请求不是欺诈性的而是可信实体。

[0029] 本发明的实施例还允许简化系统中所有令牌请求方计算机-服务提供商计算机组合的认证和数据加密密钥管理。另外，本发明的实施例提供增加的透明度，因为在预配和授权处理期间，例如TRID的令牌请求方标识符和例如TR-TSP标识符的服务提供商标识符可以

提供给授权实体。本发明的实施例还消除了令牌服务计算机向每个新的令牌请求方提供加密密钥的需要。相反，令牌服务计算机只需要向服务提供商提供加密密钥。任何安全性更新都可以由服务提供商计算机轻松处理，因为它具有预先存在的连接(例如，API)以及与其令牌请求方的关系。

[0030] 在论述本发明的一些实施例的细节之前，对一些术语的描述可用于理解各种实施例。

[0031] “用户装置”可以是可以与用户装置交互的任何合适的装置(例如，支付卡或移动电话)。用户装置可以采用任何合适的形式。用户装置的一些实例包括蜂窝电话、PDA、个人计算机(PC)、平板计算机等。在用户装置是移动装置的一些实施例中，移动装置可以包括显示器、存储器、处理器、计算机可读介质和任何其它合适的组件。

[0032] “移动装置”(有时被称作移动通信装置)可以包括用户可以运输或操作的任何电子装置。在一些情况下，移动装置还可以提供与网络的远程通信能力。移动通信装置可以使用移动电话(无线)网络、无线数据网络(例如，3G、4G或类似网络)、Wi-Fi、蓝牙、低功耗蓝牙(BLE)、Wi-Max或可以提供对例如因特网或专用网络等网络的访问的任何其它通信介质来进行通信。移动装置的实例包括移动电话(例如，蜂窝电话)、PDA、平板计算机、上网本、膝上型计算机、可穿戴装置(例如手表)、例如汽车和摩托车之类的车辆、个人音乐播放器、手持式专用阅读器等。移动装置可以包括用于执行此类功能的任何合适的硬件和软件，并且还可以包括多个装置或组件(例如，当装置通过与另一装置进行网络共享(即，使用所述另一装置作为调制解调器)而远程访问网络时，一起使用的两个装置可以被认为是单个移动装置)。

[0033] “资源提供商”可以是在交易期间提供资源(例如，商品、服务、对安全数据的访问、对位置的访问等)的任何合适的实体。例如，资源提供实体可以是商家、场所运营商、建筑物所有者、政府实体等。“商家”通常可以是参与交易且可以出售商品或服务或提供对商品或服务的取用的实体。

[0034] “应用程序”可以是用于特定目的的计算机程序。

[0035] “认证数据”可以包括适用于认证例如用户或移动装置等实体的任何数据。认证数据可以从用户或用户操作的装置获得。从用户获得的认证数据的实例可以包括个人标识号(PIN)、生物计量数据、密码等。可以从装置获得的认证数据的示例可以包括装置序列号、硬件安全元件标识符、装置指纹、电话号码、IMEI号等。

[0036] “访问装置”可以是用于提供对外部计算机系统的访问的任何合适的装置。访问装置可以呈任何合适的形式。访问装置的一些示例包括销售点(POS)装置、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用读取器、机顶盒、电子现金出纳机(ECR)、自动柜员机(ATM)、虚拟现金出纳机(VCR)、查询一体机、安全系统、访问系统、网站等等。访问装置可以使用任何合适的接触或非接触操作模式，以向移动装置发送或从其接收数据或与移动装置相关联。在访问装置可以包括POS终端的一些实施例中，可使用任何合适的POS终端并且其可以包括读取器、处理器和计算机可读介质。读取器可以包括任何合适的接触式或非接触式操作模式。例如，示例性读卡器可以包括射频(RF)天线、光学扫描仪、条形码读取器或磁条读取器，以与移动装置进行交互。

[0037] “电子钱包”或“数字钱包”可以包括允许个人进行电子商务交易的电子装置。数字

钱包可以存储用户简档信息、凭证、银行账户信息、一个或多个数字钱包标识符等，并且可以用于各种交易中，例如但不限于电子商务交易、社交网络交易、转账/个人支付交易、移动商务交易、邻近支付交易、游戏交易等。数字钱包可以设计为简化购买和支付过程。数字钱包可以允许用户将一个或多个支付卡加载到数字钱包上，以便进行支付而无需输入账号或出示实体卡。

[0038] “凭证”可以是充当价值、所有权、身份或权限的可靠证据的任何合适的信息。凭证可以是一串数字、字母或任何其它合适的字符，以及可用作确认的任何对象或文件。凭证的实例包括价值凭证、标识卡、认证文件、访问卡、口令和其它登录信息等。凭证的其它实例包括主账号(PAN)、个人可识别信息(PII)，例如姓名、地址、电话号码等。

[0039] “授权实体”可以是通常使用授权计算机来授权请求的实体。授权实体可以是发行方、政府机构、文件存储库、访问管理员等。“发行方”通常可以包括维护用户账户的商业实体(例如，银行)。发行方还可向用户发行存储在蜂窝电话、智能卡、平板电脑或笔记本电脑等用户装置上的支付凭证。

[0040] “服务提供商”可以是可提供服务的实体。服务提供商的实例包括商家、数字钱包、支付处理器、社交网络等。

[0041] “用户”可以包括个别或计算装置。在一些实施例中，用户可以与一个或多个个人账户和/或移动装置相关联。在一些实施例中，用户可以是持卡人、账户持有人或消费者。

[0042] “令牌”可以是凭证的替代值。令牌可以是一串数字、字母或任何其他合适的字符。令牌的示例包括支付令牌、访问令牌、个人标识令牌等。

[0043] “支付令牌”可包括替代主账号(PAN)等账户标识符的支付账户标识符。例如，令牌可以包括可以用作原始账户标识符的替代的一系列字母数字字符。例如，令牌“4900 0000 0000 0001”可以用于代替PAN“4147 0900 0000 1234”。在一些实施例中，令牌可以是“保持格式的”，并可以具有与现有交易处理网络中使用的账户标识符一致的数字格式(例如ISO 8583金融交易消息格式)。在一些实施例中，令牌可以代替PAN用来发起、授权、处理或解决支付交易，或者在通常将提供原始凭证的其他系统中表示原始凭证。在一些实施例中，可生成令牌值，使得可能无法以计算方式从令牌值得到原始PAN或其他账户标识符的恢复。此外，在一些实施例中，令牌格式可以被配置成允许接收令牌的实体将其标识为令牌，并识别发行令牌的实体。

[0044] “密钥”可以包括在密码算法中用于将数据变换成另一表示的一条信息。密码算法可以是将原始数据变换成替代表示的加密算法，或将加密信息变换回到原始数据的解密算法。密码算法的实例可包括三重数据加密标准(TDES)、数据加密标准(DES)、高级加密标准(AES)等。

[0045] “授权请求消息”可以是可用于请求授权某事的消息。在一些实施例中，授权请求消息可以是发送给支付处理网络和/或支付卡的发行方以请求授权交易的电子消息。根据一些实施例的授权请求消息可符合ISO8583，这是针对交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息可以包括可与支付装置或支付账户相关联的发行方账户标识符。授权请求消息还可以包括对应于“标识信息”的额外数据元素，仅作为实例包括：服务代码、CVV(卡验证值)、dCVV(动态卡验证值)、到期日期等。授权请求消息还可包括“交易信息”，例如与当前交易相关联的任何信息，例如交易量、

商家标识符、商家位置等，以及可用于确定是否标识和/或授权交易的任何其它信息。

[0046] “授权响应消息”可以是对授权请求消息的电子消息回复。在一些情况下，授权响应消息由发行金融机构或支付处理网络生成。授权响应消息可以包括(只作为示例)以下状态指示符中的一个或多个：批准-交易被批准；拒绝-交易未被批准；或呼叫中心-响应未决的更多信息，商家必须呼叫免费授权电话号码。授权响应消息还可以包括授权代码，其可以是信用卡发行银行响应于电子消息中的授权请求消息(直接地或通过支付处理网络)返回给商家的访问装置(例如，POS设备)的指示交易被批准的代码。所述代码可以用作授权的证据。如上所述，在一些实施例中，支付处理网络可向商家生成或转发授权响应消息。

[0047] “服务器计算机”通常是功能强大的计算机或计算机集群。例如，服务器计算机可以是大型主机、小型计算机集群或充当单元的一组服务器。在一个示例中，服务器计算机可以是耦合到网络服务器的数据库服务器。

[0048] “处理器”可以包括任何合适的一个或多个数据计算装置。处理器可以包括一起工作以实现期望的功能的一个或多个微处理器。处理器可以包括CPU，所述CPU包括至少一个高速数据处理器，所述高速数据处理器足以执行用于执行用户和/或系统生成的请求的程序成分。CPU可以是微处理器，例如AMD的Athlon、Duron和/或Opteron；IBM和/或Motorola的PowerPC；IBM和Sony的Cell处理器；Intel的Celeron、Itanium、Pentium、Xeon和/或XScale；和/或类似的处理器。

[0049] “存储器”可以是能够存储电子数据的任何合适的一个或多个装置。合适的存储器可包括非瞬态计算机可读介质，其存储可由处理器执行以实现所要方法的指令。存储器的实例可以包括一个或多个存储器芯片、磁盘驱动器等。此类存储器可使用任何合适的电、光和/或磁操作模式来操作。

[0050] “令牌服务计算机”可以是用于生成、管理和提供令牌的任何计算机、计算机群组或计算机网络。

[0051] “令牌请求方”可以是需要来自令牌服务计算机的令牌的任何实体。作为令牌请求方的实体可以包括商家、市场、收单方、支付服务提供商、数字钱包等。

[0052] 例如TRID的“令牌请求方标识符”可以是用于唯一地标识令牌请求方的任何类型的指示符。

[0053] “服务提供商标识符”可以是操作服务提供商计算机的服务提供商的标识符。在一些实施例中，服务提供商标识符可以被称为TR-TSP标识符。

[0054] “交互信道”是两个或更多个方可以通过其进行交互的信道。交互信道可以是通过其安全地完成交易的支付信道，例如卡呈现信道、电子商务信道、电话信道等。

[0055] 图1示出了包括服务提供商计算机105以及与服务提供商计算机105通信的令牌请求方110A-110C的示例系统100。每个令牌请求方110A-110C可以是令牌请求方计算机或操作令牌请求方计算机。此处，服务提供商计算机105可以是令牌请求方-令牌服务提供商(TR-TSP)，并且令牌请求方110A-C可以是使用TR-TSP作为服务提供商的资源提供商(例如，商家)。每个令牌请求方110A-C都可以具有唯一令牌请求方标识符(TRID)，所述TRID可以用于在交易期间标识令牌请求方110A-C。此TRID可以由服务提供商计算机105或令牌服务计算机107提供给令牌请求方110A-C。示例TRID值可以从可用于将其标识为TRID的值开始，然后可以后接形成对于令牌请求方110A-C唯一的标识符的任何数目的值。例如，TRID值可以

从用以将其标识为TRID的数字“400”开始，这些数字可以后接八个额外数字作为唯一标识符。

[0056] 服务提供商计算机105可以通过令牌服务计算机107提供的API向令牌服务计算机107注册令牌请求方110A-110C。在注册过程中，令牌服务计算机107可以定义服务提供商计算机105和令牌请求方110A-110C的角色与职责。服务提供商计算机105还可以获得关于每个令牌请求方110A-110C的具体细节。例如，令牌请求方计算机可能需要提供外部客户端ID(例如，由与向令牌服务计算机标识令牌请求方的令牌请求方计算机相关联的服务提供商计算机提供的ID)，令牌请求方标识符(TRID)(例如，由令牌服务计算机分配的令牌请求方ID，如果可用的话)，与令牌请求方相关联的名称(例如，商品名称、法定名称等)，应用程序URL(例如，令牌请求方计算机的应用程序网站URL)，令牌请求方操作所在的国家的国家代码(例如，ISO国家代码)，DUN ID(例如，由Dun和Bradstreet分配的ID)，收单方分配的商家ID(例如，由与商家相关联的收单方分配的用以向收单方标识商家的ID)，和/或政府ID(例如，税务ID)。

[0057] 图2示出了说明服务提供商计算机210使用令牌服务计算机220向授权实体计算机240注册令牌请求方ID(TRID)的系统和过程流程的图式。如上文关于图1所描述，服务提供商计算机210可以与使用唯一TRID的数个令牌请求方或令牌请求方计算机相关联。TRID报告数据库230可以是令牌服务计算机220可以在其中存储TRID值和TRID报告信息的数据库。TRID报告数据库230可以由令牌服务计算机220和授权实体计算机240两者访问。授权实体计算机240可以是例如银行的实体。

[0058] 方法可以关于图2进行描述。在步骤S201中，所述服务提供商计算机210可以经由专用注册API向令牌服务计算机220注册令牌请求方。注册过程可以将TRID分配给与服务提供商计算机210相关联的令牌请求方。在一些实施例中，令牌请求方可以是例如商家等资源提供商，且服务提供商计算机210可以是数字钱包计算机或社交网络计算机。

[0059] 在步骤S202中，在接收到注册令牌请求方的请求之后，令牌服务计算机220可以将TRID通知发送到授权实体计算机240。在步骤S203中，令牌服务计算机220还可以将TRID值和与其相关联的任何信息存储在TRID报告数据库230中。TRID报告数据库230可以存储例如分配给令牌请求方的TRID、例如分配给服务提供商计算机230的TR-TSP标识符的服务提供商标识符、令牌请求方的法定名称等信息。

[0060] 在步骤S204中，授权实体240可以访问TRID报告230数据库中的任何信息。

[0061] 图3示出了具有与服务提供商计算机305和令牌服务计算机307通信的令牌请求方计算机310A-310C的系统300。每个令牌请求方计算机310A-310C可以从令牌服务计算机330请求令牌和/或交易密码。服务提供商计算机320可以与令牌服务计算机330形成可信关系，而不是为每个令牌请求方计算机310A-310C生成唯一的加密密钥来加密发送到令牌服务计算机330和从所述令牌服务计算机接收到的消息。由于这种可信关系，令牌服务计算机330可以将单个加密密钥发到服务提供商计算机320。单个加密密钥可以被称为加密超级密钥(ESK)，其可以用于加密服务提供商计算机320与令牌服务计算机330之间的所有通信，而不考虑与通信有关的令牌请求方计算机310A-310C。令牌请求方计算机310A-310C与服务提供商计算机305之间的通信可以使用相应的密钥对CK1-CK1’、CK2-CK2’、CK3-CK3’来加密。密钥对CK1-CK1’、CK2-CK2’、CK3-CK3’可以是对称或非对称密码密钥对。

[0062] 示意性地，第一令牌请求计算机310A可以经由服务提供商计算机305从令牌服务计算机307请求令牌。从第一令牌请求方计算机310A到服务提供商计算机305的通信可以由第一令牌请求方计算机310A用密钥CK1加密，并且可以由服务提供商计算机305用密钥CK1'解密。从服务提供商计算机305到令牌服务计算机307的通信可以由服务提供商计算机305用密钥ESK加密，并且可以由令牌服务计算机307用密钥ESK'解密。然后，令牌服务计算机307可以处理令牌请求。

[0063] 在另一时间，第二令牌请求计算机310B可以经由服务提供商计算机305从令牌服务计算机307请求令牌。从第二令牌请求方计算机310B到服务提供商计算机305的通信可以由第一令牌请求方计算机310A用密钥CK2加密，并且可以由服务提供商计算机305用密钥CK2'解密。从服务提供商计算机305到令牌服务计算机307的通信可以由服务提供商计算机305用密钥ESK加密，并且可以由令牌服务计算机307用密钥ESK'解密。然后，令牌服务计算机307可以处理令牌请求。

[0064] 令牌服务计算机330可以创建服务提供商计算机与令牌请求方关系的映射。可以通过映射与服务提供商计算机320相关联的例如TR-TSP标识符的服务提供商标识符和与可信TR-TSP标识符相关联的令牌请求方计算机310A-310C的TRID之间的关联来创建表。令牌服务计算机330接着可生成新的加密密钥，所述新的加密密钥将被接受作为加密超级密钥，并授权访问由服务提供商计算机320提供的通信。然后，令牌服务计算机330可以允许用加密超级密钥来认证请求。加密超级密钥可以具有任何合适类型的加密密钥(例如，AES256、RSA PKI 2048、不透明度A、ECC等)，并且可以允许任何认证散列类型(例如，SHA256(x)、HmAC(xv2)等)。

[0065] 应注意，图3中示出且关于图3进行描述的加密密钥方案可以用于在图4-7中的任一过程流程中加密或解密来自类似实体的消息，所述过程流程在下文中进行描述。例如，关于图6，在步骤S602中，消息可以用例如CK1的密钥加密，然后用例如CK1的密钥解密。随后在步骤S603中，已解密消息可以用密钥ESK加密，然后用对应的密钥ESK解密。

[0066] 图4示出了用于将电子商务(E-Com)/存档凭证(COF)令牌预配到与资源提供商计算机410相关联的资源提供商的示例性过程流程400。资源提供商计算机410可以是和与令牌服务计算机430通信的服务提供商计算机20相关联的令牌请求方计算机。

[0067] 在步骤S401中，服务提供商计算机420可以向令牌服务计算机430发送针对资源提供商计算机410(例如，商家计算机)的电子商务(E-Com)/存档凭证(COF)令牌的令牌请求消息。令牌请求消息可以包括主账号(PAN)或对PAN的引用、与服务提供商计算机420相关联的服务提供商计算机标识符(例如，TR-TSP标识符)以及与资源提供商计算机410相关联的TRID。

[0068] 在步骤S402中，令牌服务计算机430可以验证服务提供商计算机420与资源提供商计算机410之间的关系。然后，在验证后，令牌服务计算机430可以将令牌请求消息发送至授权实体计算机440。

[0069] 在步骤S403中，授权实体计算机440可以通过批准或拒绝请求来响应于令牌请求消息。授权实体计算机440可以将令牌响应发送回令牌服务计算机530。

[0070] 在步骤S404中，在从授权实体440接收到批准通知后，令牌服务计算机430可以生成具有与资源提供商计算机410相关联的TRID的E-Com/COF令牌，并继续到步骤S405。如果

令牌服务计算机430从授权实体440接收到拒绝通知，则令牌服务计算机430可以生成被拒令牌响应消息并跳到步骤S406。

[0071] 在步骤S405中，令牌服务计算机430可以将令牌创建通知发送到授权实体计算机440，所述通知包括适当的令牌数据。然后，令牌服务计算机430可以在表中将服务提供商计算机标识符映射到令牌请求方标识符和所发出令牌。

[0072] 在步骤S406中，令牌服务计算机430可以向服务提供商计算机420发送包含E-Com/COF令牌或拒绝通知的令牌响应消息。在一些实施例中，服务提供商计算机420可以代表资源提供商计算机410存储接收到的令牌以用于未来交易。

[0073] 在步骤S407中，服务提供商计算机420可以将从令牌服务计算机430接收到的令牌响应消息转发到资源提供商计算机410。资源提供商计算机410接收到的令牌响应消息可以包含或可以不包含令牌。

[0074] 图5示出了用于将令牌预配到使用现有装置令牌的资源提供商计算机510的示例性过程流程500。资源提供商计算机510可以是与服务提供商计算机520相关联的令牌请求方。

[0075] 在步骤S501中，服务提供商计算机520向令牌服务计算机530发送针对资源提供商的E-Com/COF令牌的令牌请求消息。令牌请求消息可以至少包括与资源提供商计算机510相关联的令牌、与服务提供商计算机520相关联的服务提供商计算机标识符(例如，TR-TSP标识符)以及与资源提供商计算机510相关联的TRID。另外，令牌请求消息还可以包括与资源提供商计算机510相关联的密码。

[0076] 在步骤S502中，如果装置密码存在于令牌请求消息中，则令牌服务计算机530可以验证资源提供商计算机510的密码。在验证后，令牌服务计算机530可以将令牌请求消息发送到授权实体计算机540。令牌请求消息可以数字消息(例如，0100TAR/AV消息)的形式发送到授权实体计算机540。消息可以至少包含以下信息：PAN、PAN源、与资源提供商计算机510相关联的TRID、以及与服务提供商计算机520相关联的服务提供商标识符。

[0077] 在步骤S503中，授权实体计算机540可以通过批准或拒绝请求来响应于令牌请求消息，并且可以将响应发送回到令牌服务计算机530。

[0078] 在步骤S504中，在从授权实体计算机540接收到批准通知后，令牌服务计算机530可以针对与资源提供商计算机510相关联的TRID生成E-Com/COF令牌，并继续到步骤S505。如果令牌服务计算机530从授权实体计算机540接收到拒绝通知，则令牌服务计算机530可以生成被拒令牌响应消息并跳到步骤S506。

[0079] 在步骤S505中，令牌服务计算机530可以将令牌创建通知发送到授权实体计算机540，所述通知包括适当的令牌数据。然后，令牌服务计算机530可以将服务提供商计算机标识符与令牌请求方标识符映射到表中。

[0080] 在步骤S506中，令牌服务计算机530可以向服务提供商计算机520发送包含E-Com/COF令牌或拒绝通知的令牌响应消息。服务提供商计算机520可以存储令牌或可以将其传递到资源提供商计算机510。

[0081] 在步骤S507中，服务提供商计算机520可以将从令牌服务计算机530接收到的令牌响应消息转发到资源提供商计算机510。

[0082] 图6示出了用于用现有的存储令牌执行用户发起的交易支付的示例性过程流程

600。用户610可以是试图与和资源提供商计算机620相关联的资源提供商进行交易的任何人或实体。资源提供商计算机620可以是和与令牌服务计算机640通信的服务提供商计算机630相关联的令牌请求方。

[0083] 在步骤S601中，用户610确认其交易并通过其用户装置向资源提供商计算机620提交结账请求。交易可以是用户610与资源提供商620之间的交换。

[0084] 在步骤S602中，资源提供商计算机620将交易发起消息发送到服务提供商计算机630。交易发起消息可以包括交易期间要转移的金额、对被交换的商品或服务的描述等。

[0085] 在步骤S603中，服务提供商计算机630可以将包括令牌或令牌标识符的密码请求消息、与资源提供商相关联的资源提供商标识符以及与服务提供商计算机相关联的服务提供商计算机标识符发送到令牌服务计算机640。在一些实施例中，资源提供商标识符可以是令牌请求方ID(TRID)，并且服务提供商计算机标识符可以是令牌请求方-令牌服务提供商(TR-TSP)标识符。在一些情况下，密码请求消息可以包括令牌，例如支付令牌。可以从真实凭证(例如，PAN)以数学方式生成令牌。在其它实施例中，不提供令牌，但提供令牌标识符。令牌标识符可以用于检取由服务提供商计算机630存储的令牌，并且可以用于随后处理交易。

[0086] 在步骤S604中，令牌服务计算机640可以生成密码(例如，TAVV密码)，并且可以将步骤S603中调用的令牌和密码传回到服务提供商计算机630。密码可以是信道特定密码，以使得密码对于单个信道有效并且无法通过其它交互信道使用。令牌服务计算机640可以在生成密码之前验证令牌或与给定令牌标识符相关联的令牌、与资源提供商相关联的资源提供商标识符和服务提供商计算机标识符彼此相关联。令牌服务计算机640可以将服务提供商计算机标识符与令牌请求方标识符映射到表中。所述表存储服务提供商(TR-TSP)与资源提供商(TR)之间的关系，然后可以访问所述表以在其它交易中验证TR-TSP与TR之间的关系。

[0087] 在步骤S605中，由服务提供商计算机640将包括令牌和密码的授权请求消息发送到处理计算机660。

[0088] 在步骤S606中，处理计算机660结合令牌服务计算机640来确定与令牌相关联的真实凭证，并验证密码以确定交易是否在正确的交互信道中进行。

[0089] 在步骤S607中，处理计算机660接着会将授权响应消息发送到授权实体计算机650。

[0090] 在步骤S608中，授权实体计算机650将授权响应消息发送回到处理计算机660。

[0091] 在步骤S609中，处理计算机660交换令牌的真实凭证。

[0092] 在步骤S610中，处理计算机660将授权响应发送回到服务提供商计算机630。

[0093] 在步骤S611中，服务提供商计算机630可以将授权响应消息发送回到资源提供商计算机620。

[0094] 在步骤S612中，可以通过用户的装置将结账完成消息发送到用户610。

[0095] 稍后，可以在授权实体计算机650、处理计算机660和服务提供商计算机630或与资源提供商计算机620或服务提供商计算机630相关联的另一实体(例如，收单方计算机)之间执行清算和结算过程。

[0096] 图7示出了用于执行资源提供商发起的交易的示例性过程流程700。资源提供商计

算机710可以是和与令牌服务计算机730合作的服务提供商计算机相关联的令牌请求方。传输计算机720可以由收单方操作，并且可以针对令牌请求方处理交易。授权实体计算机740可以由例如银行的实体操作。

[0097] 在步骤S701中，资源提供商计算机710可以将授权请求消息发送到传输计算机720。

[0098] 在步骤S702中，传输计算机720可以将授权请求消息发送到令牌服务计算机730。授权请求消息可以至少包括与资源提供商计算机710相关联的令牌、与向令牌服务计算机730注册的服务提供商计算机相关联的服务提供商计算机ID，以及与资源提供商计算机710相关联的资源提供商标识符。

[0099] 在步骤S703中，令牌服务计算机730可以将在授权请求消息中发送的数据去令牌化，执行域控制，并在发送到授权实体计算机740以供批准的授权请求消息中填入任何相关标签。

[0100] 在步骤S704中，授权实体计算机740可以批准或拒绝交易，并且可以将授权响应消息发送回到令牌服务计算机730。

[0101] 在步骤S705中，令牌服务计算机730可以将授权响应消息发送到服务提供商计算机720。

[0102] 在步骤S706中，传输计算机720可以将授权响应消息发送到资源提供商计算机710。

[0103] 稍后，可以在授权实体计算机740、处理计算机和服务提供商计算机720或与资源提供商计算机710或服务提供商计算机720相关联的另一实体(例如，收单方计算机)之间执行清算和结算过程。图8示出了根据本发明的实施例的服务提供商计算机800的框图。图8示出了服务器计算机800A和耦合到服务器计算机800A的数据库800B。

[0104] 数据库800B可以存储与其正进行交互的每个令牌请求方(例如，资源提供商)和令牌服务计算机相关联的账户信息。所述数据库还可以存储先前描述的密码密钥，所述密码密钥用于保护资源提供商与令牌服务计算机之间的通信。

[0105] 数据库800B(以及本文所描述的任何其它数据库)可以是常规的、容错的、关系的、可扩展的、安全的数据库，例如Oracle™或Sybase™。数据库800B可以使用例如阵列、散列、(链接)列表、结构化文本文件(例如，XML)、表等的各种标准数据结构来实施。此类数据结构可以存储在存储器和/或(结构化的)文件中。

[0106] 服务器计算机800A可以包括处理器801，所述处理器可以耦合到系统存储器802和外部通信接口803。计算机可读介质804也可以可操作地耦合到处理器801。

[0107] 计算机可读介质804可以包括数个软件模块，包括通信模块804A、加密模块804B、数据库更新模块804C、认证码生成模块804D、授权模块804E和验证模块804F。

[0108] 通信模块804A可以包括使得处理器801生成消息、转发消息、重新格式化消息和/或以其它方式与其它实体进行通信的代码。

[0109] 在本发明的实施例中，加密模块804B可以包括用于加密数据的任何合适的加密算法。合适的数据加密算法可包括DES、三重DES、AES等。其还可以存储加密密钥，这些加密密钥可以与此类加密算法一起使用。加密模块804B可以利用对称或不对称加密技术来加密和/或验证数据。

[0110] 数据库更新模块804C可以结合处理器801一起工作，以更新数据库800B中的账户信息。

[0111] 路由模块804D可以包括计算机代码，所述计算机代码在由处理器801执行时使得服务提供商计算机800适当地将消息路由到其预期目的地。

[0112] 授权模块804E可以包括代码，所述代码可使得处理器801执行包括生成和发送授权请求和响应消息的授权处理。

[0113] 验证模块804F可以包括代码，所述代码使得处理器801验证任一令牌请求方。

[0114] 计算机可读介质804可以包括代码，所述代码可由处理器执行以实施一种方法，包括：从资源提供商计算机接收交易发起消息；向令牌服务计算机发送包括令牌或令牌标识符，与资源提供商相关联的资源提供商标识符和与服务提供商计算机相关联的服务提供商计算机标识符的密码请求消息；响应于发送密码请求消息，接收包括令牌和密码的密码响应消息；生成包括令牌和密码的授权请求消息；向与令牌服务计算机通信的处理计算机发送授权请求消息，其中处理计算机结合令牌服务计算机来确定与令牌相关联的真实凭证并验证密码；以及响应于发送授权请求消息，从处理计算机接收授权响应消息。

[0115] 图9示出了根据实施例的令牌服务计算机900的框图。在本发明的一些实施例中，令牌服务计算机900还可在支付处理网络中。令牌服务计算机900可以包括处理器901，所述处理器可以耦合到系统存储器902和外部通信接口903。计算机可读介质904也可以可操作地耦合到处理器901。

[0116] 在一些实施例中，令牌服务计算机900可以是支付处理网络的一部分，其在发行方与收单方之间切换交易请求和响应。支付处理网络可以是交易处理网络。交易处理网络可以处理支付交易或其他类型的访问交易。

[0117] 计算机可读介质904可以包括数个软件模块，包括通信模块904A、令牌模块904B、验证模块904C和加密模块904D。

[0118] 通信模块904A可以包括使得处理器901生成消息、转发消息、重新格式化消息和/或以其它方式与其它实体进行通信的代码。

[0119] 令牌模块904B可以包括使得处理器901获得和/或管理令牌的代码。所述令牌模块可以包括用于以数学方式导出令牌或从存储器或外部源获得令牌的代码。

[0120] 验证模块904C可以包括用以执行风险分析或验证令牌请求方或服务提供商的代码。例如，验证模块904C结合处理器901一起可以评估关于令牌请求方、服务提供商以及与令牌相关联的凭证的数据，以确定向令牌请求方提供令牌存在的风险是否高得不可接受。

[0121] 加密模块904D可以包括使得处理器901执行加密处理的代码。合适的数据加密算法可包括DES、三重DES、AES等。其还可以存储加密密钥，这些加密密钥可以与此类加密算法一起使用。

[0122] 处理器901还可以与数据库906进行通信。数据库906可以包括链接令牌请求方标识符、令牌、真实凭证和服务提供商标识符的记录。数据库906还可以存储令牌、密码、密码密钥等。

[0123] 本发明的实施例不限于上文所描述的实施例。上文提供关于上文所描述的一些方面的特定细节。可以在不脱离本发明的实施例的精神和范围的情况下以任何合适方式组合具体方面的具体细节。举例来说，在本发明的一些实施例中，后端处理、数据分析、数据收集

以及其它交易可以全部组合。然而，本发明的其它实施例可以涉及与每个个别方面或这些个别方面的特定组合相关的特定实施例。

[0124] 应理解，如上文所描述的本发明可以模块化或一体化方式使用计算机软件(存储在有形物理介质中)以控制逻辑的形式实施。基于本公开和本文中所提供的教示，本领域的普通技术人员将知晓并且了解使用硬件和硬件与软件的组合来实施本发明的其它方式和/或方法。

[0125] 本申请中描述的任何软件组件或功能可以使用例如常规的或面向对象的技术并使用任何合适的计算机语言(例如Java、C++或Perl)实施为待由处理器执行的软件代码。软件代码可以存储为计算机可读介质，例如随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质，或例如CD-ROM的光学介质上的一系列指令或命令。任何此类计算机可读介质可驻存在单个计算设备上或单个计算设备内，并且可以存在于系统或网络内的不同计算设备上或不同计算设备内。

[0126] 以上描述是说明性的并且不是限制性的。在阅读了本公开之后，本发明的许多变型形式对于本领域的技术人员将变得显而易见。因此，本发明的范围不应当参考上面的描述来确定，而是应当参考未决的权利要求连同其完整范围或等同物来确定。

[0127] 在不脱离本发明的范围的情况下，任何实施例的一个或多个特征可与任何其它实施例的一个或多个特征组合。

[0128] 除非具体地相反指示，否则“一(a/an)”或“所述(the)”的叙述打算意指“一个或多个”。

[0129] 上文提及的所有专利、专利申请、公开案和描述都出于所有目的以全文引用的方式并入本文中。并非承认它们是现有技术。

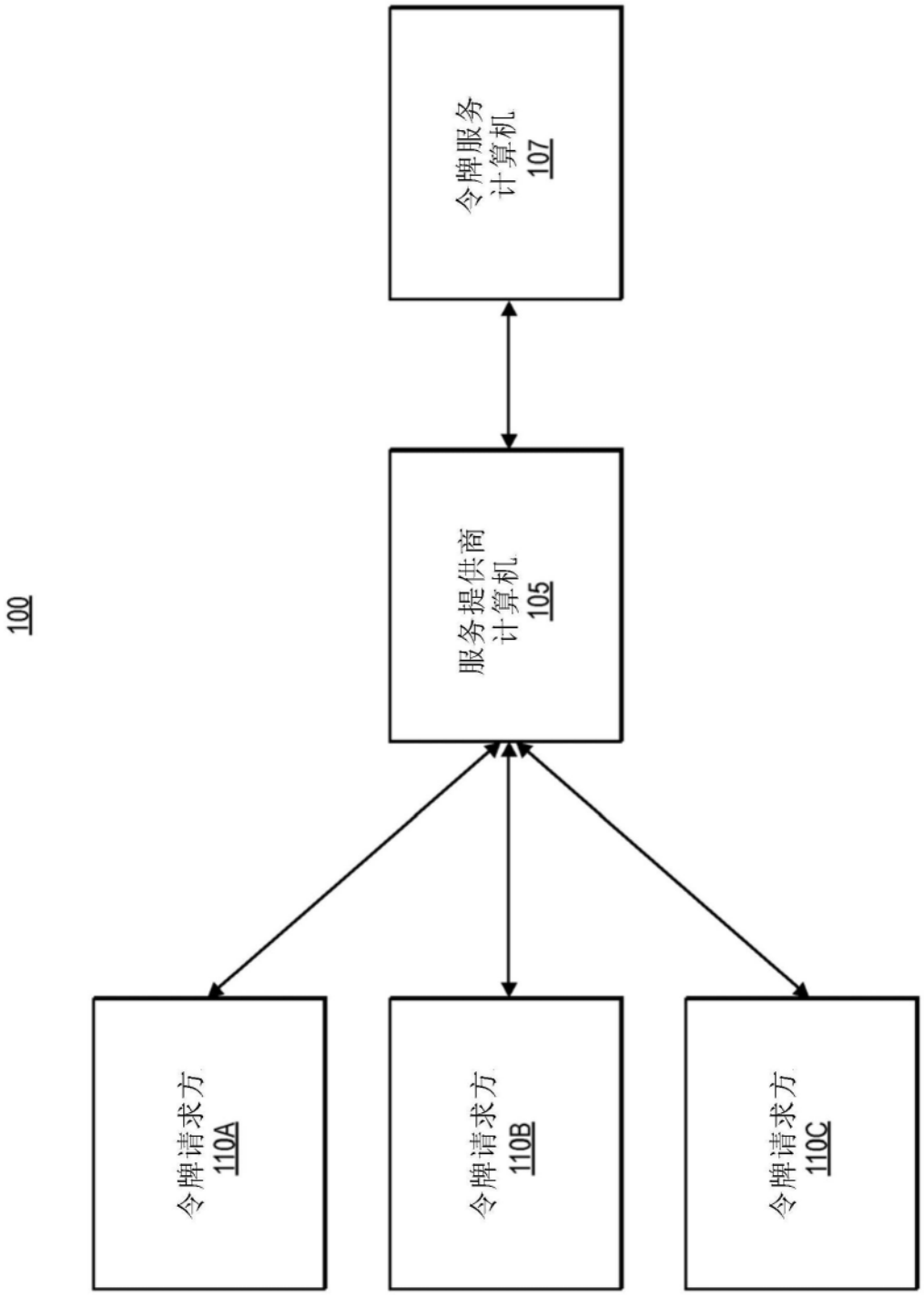

100
令牌服务
计算机
107
服务提供商
计算机
105
令牌请求方
110A
令牌请求方
110B
令牌请求方
110C

图1

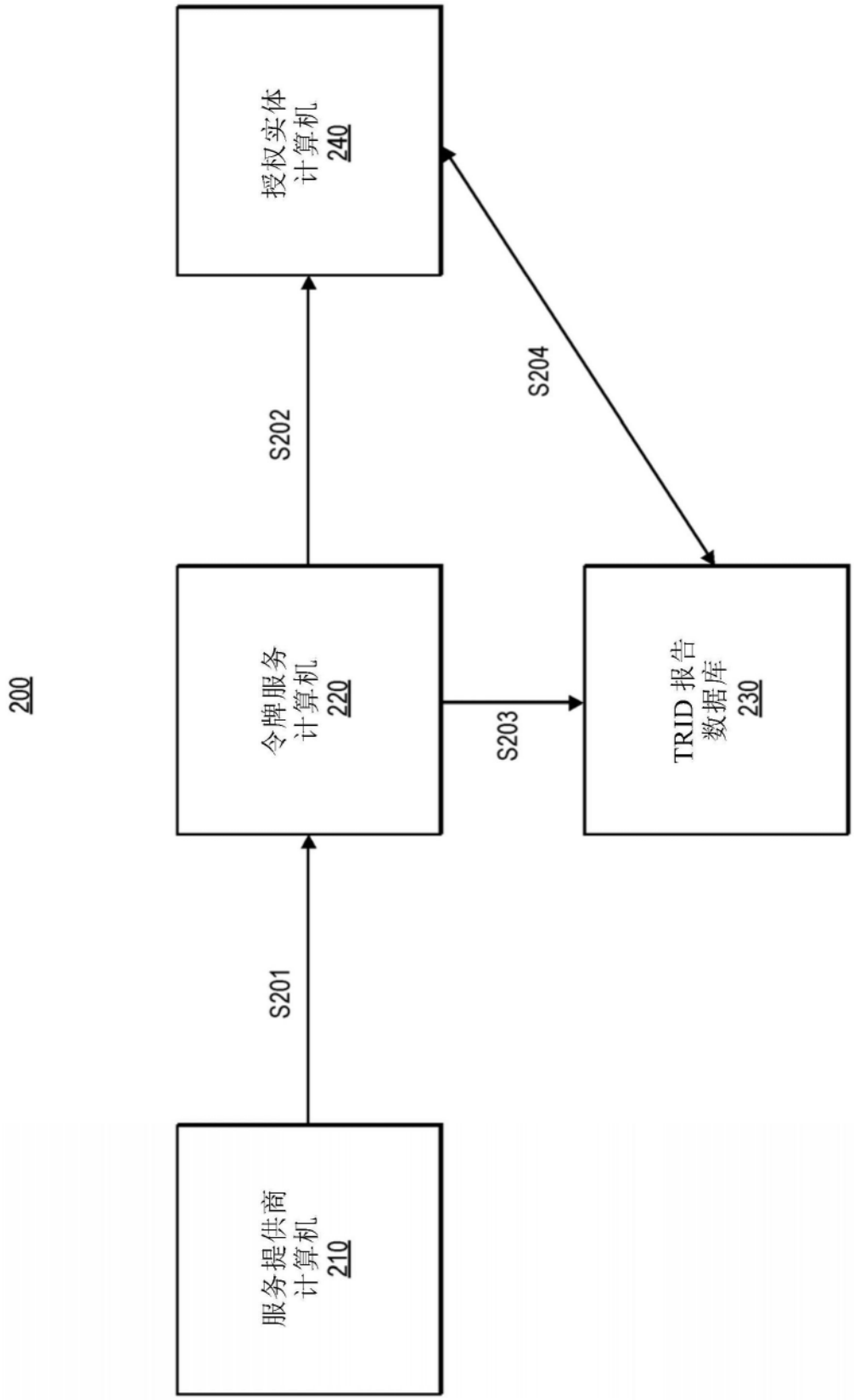

200
服务提供商
计算机
210
令牌服务
计算机
220
授权实体
计算机
240
TRID 报告
数据库
230
S201
S202
S203
S204

图2

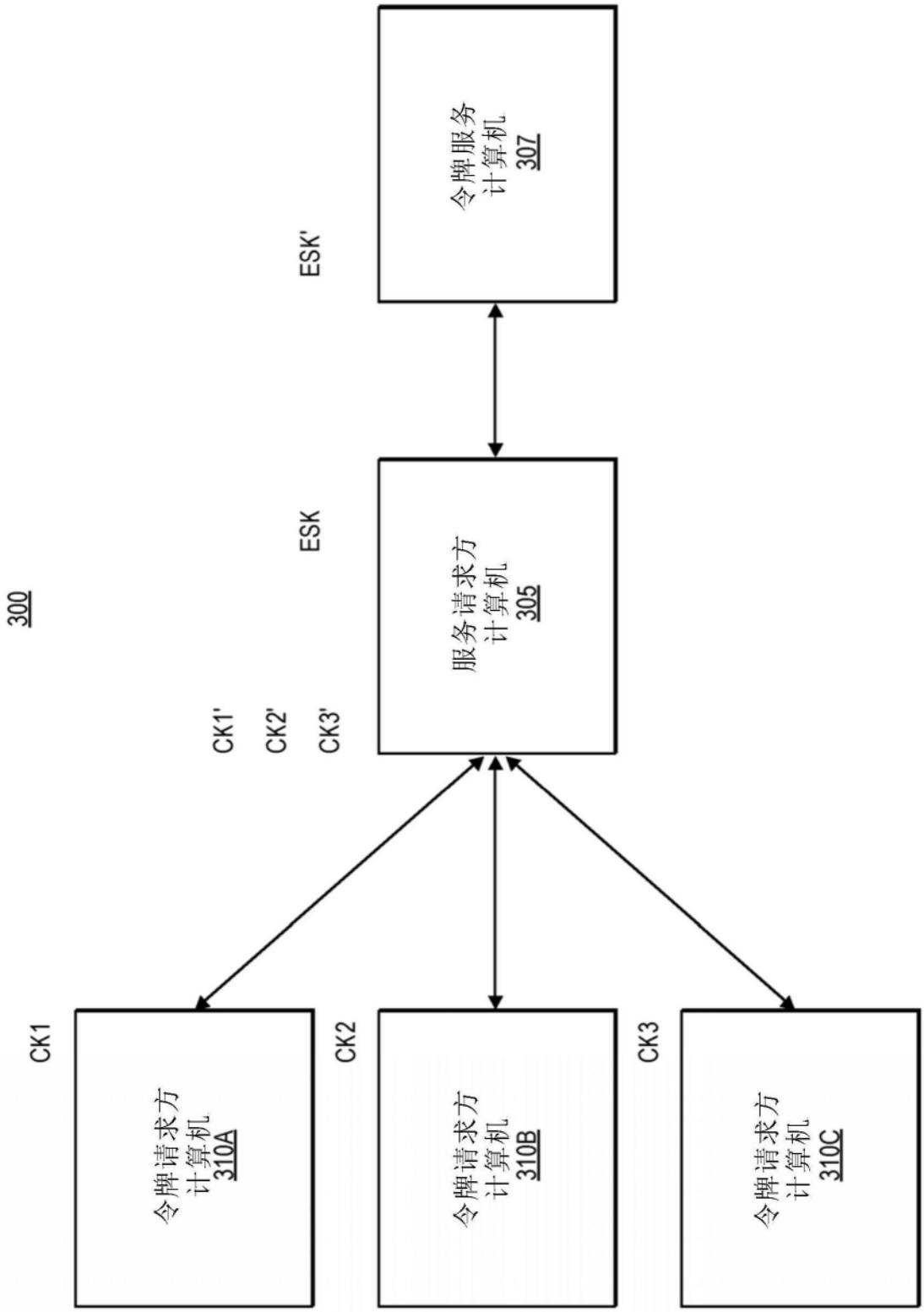

300
令牌服务
计算机
307
ESK'
ESK
服务请求方
计算机
305
CK1'
CK2'
CK3'
CK1
令牌请求方
计算机
310A
CK2
令牌请求方
计算机
310B
CK3
令牌请求方
计算机
310C

图3

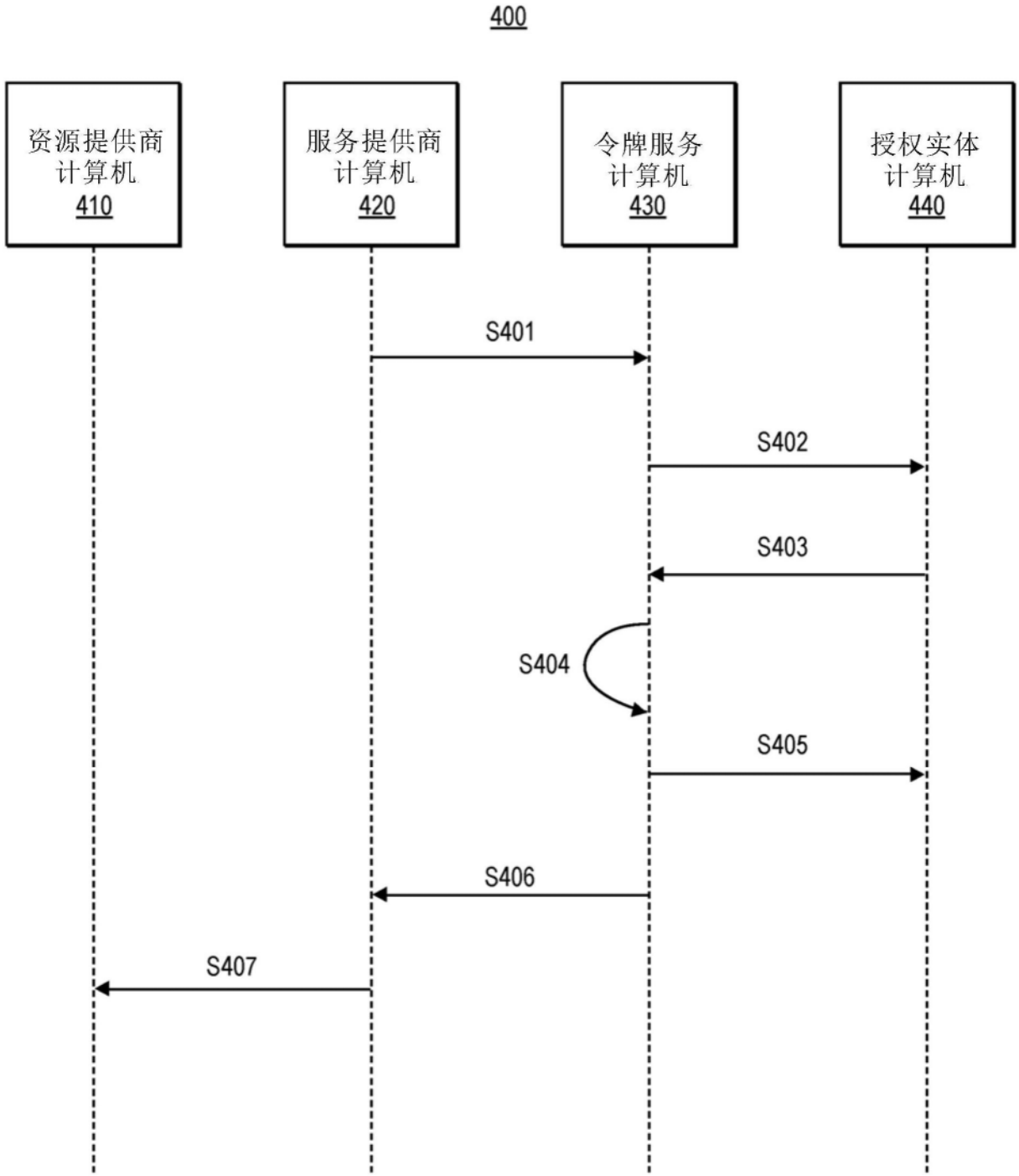

400
资源提供商计算机 410
服务提供商计算机 420
令牌服务计算机 430
授权实体计算机 440
S401
S402
S403
S404
S405
S406
S407

图4

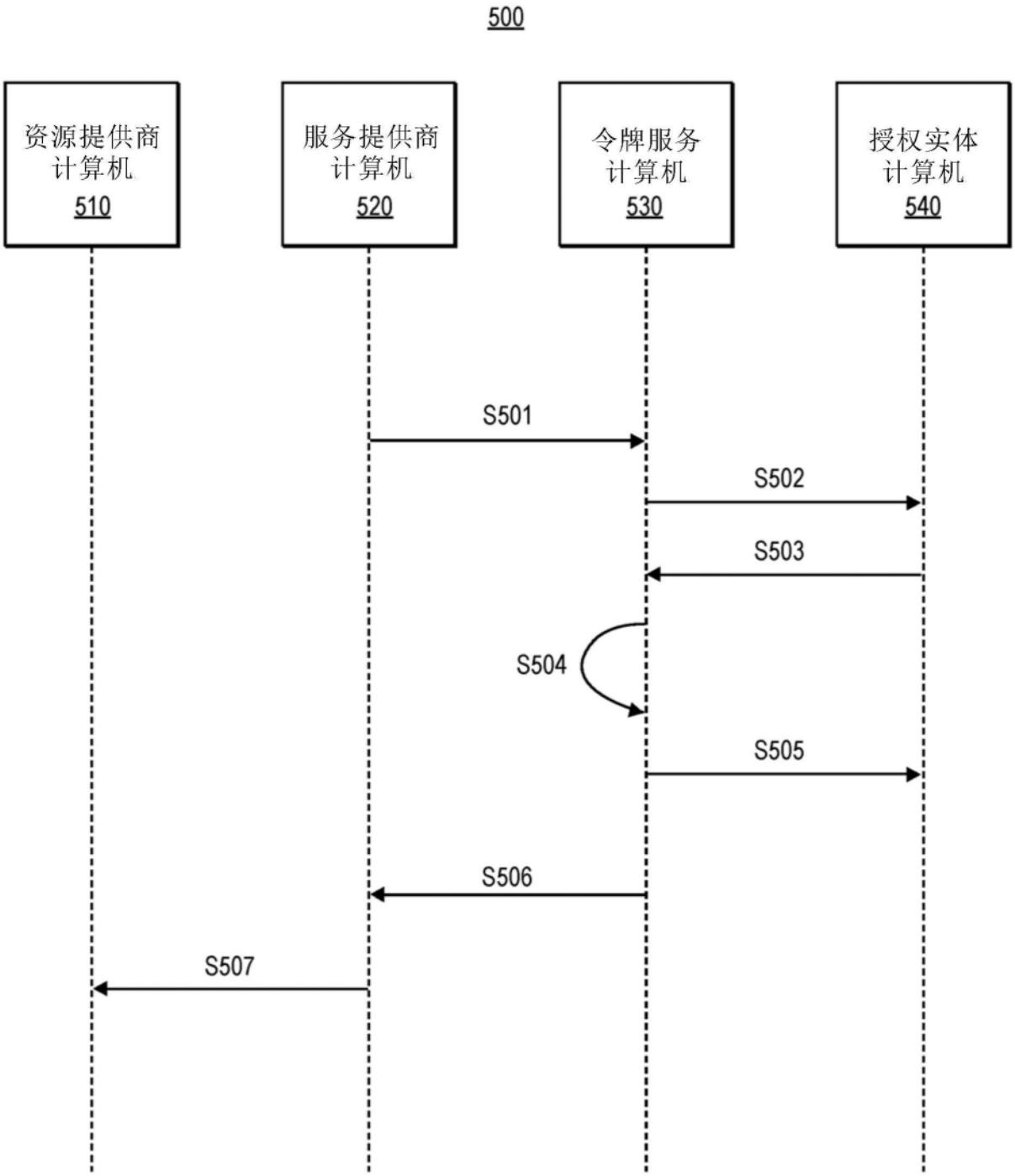

500
资源提供商计算机
510
服务提供商计算机
520
令牌服务计算机
530
授权实体计算机
540
S501
S502
S503
S504
S505
S506
S507

图5

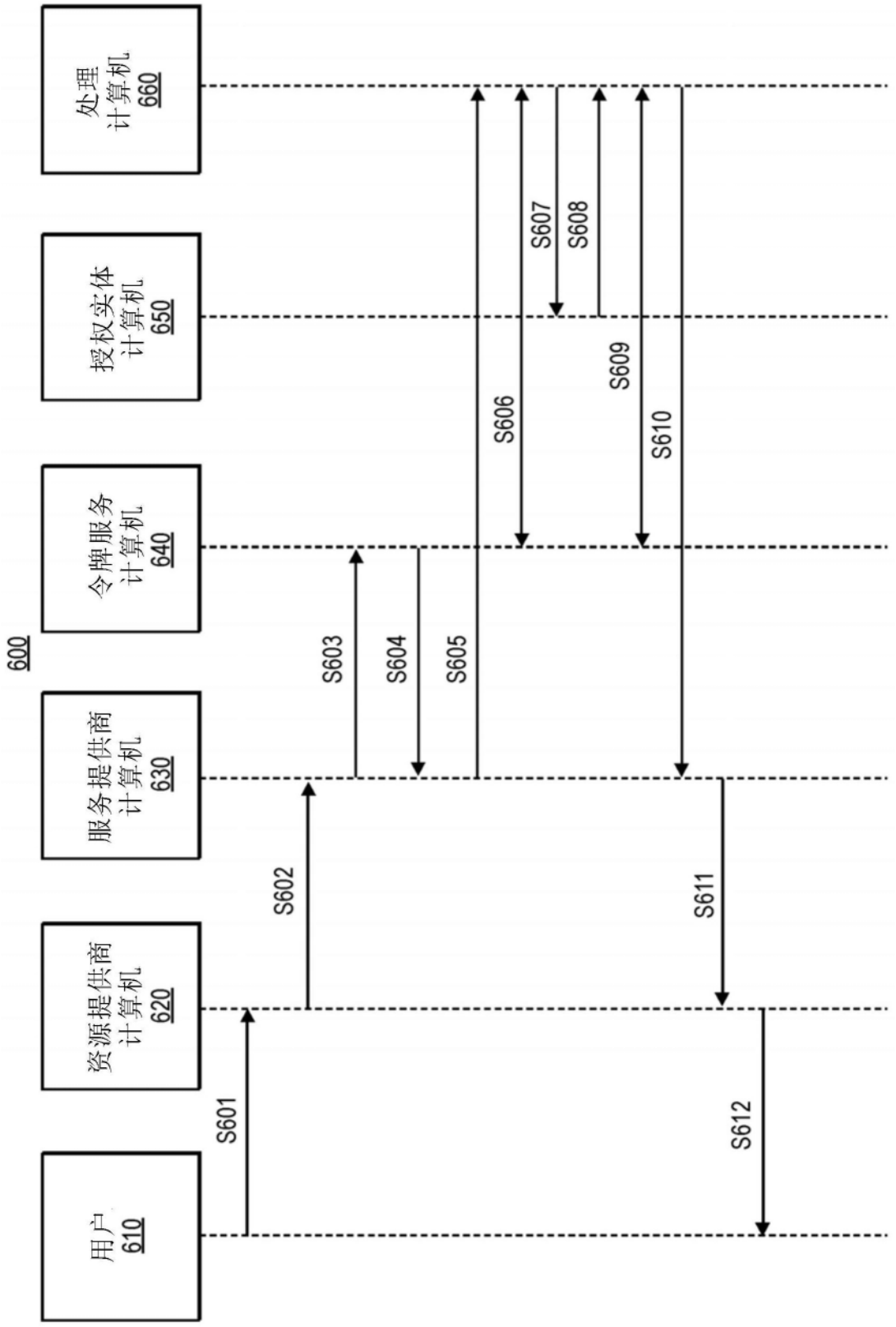

600
用户 610
资源提供商计算机 620
服务提供商计算机 630
令牌服务计算机 640
授权实体计算机 650
处理计算机 660
S601
S602
S603
S604
S605
S606
S607
S608
S609
S610
S611
S612

图6

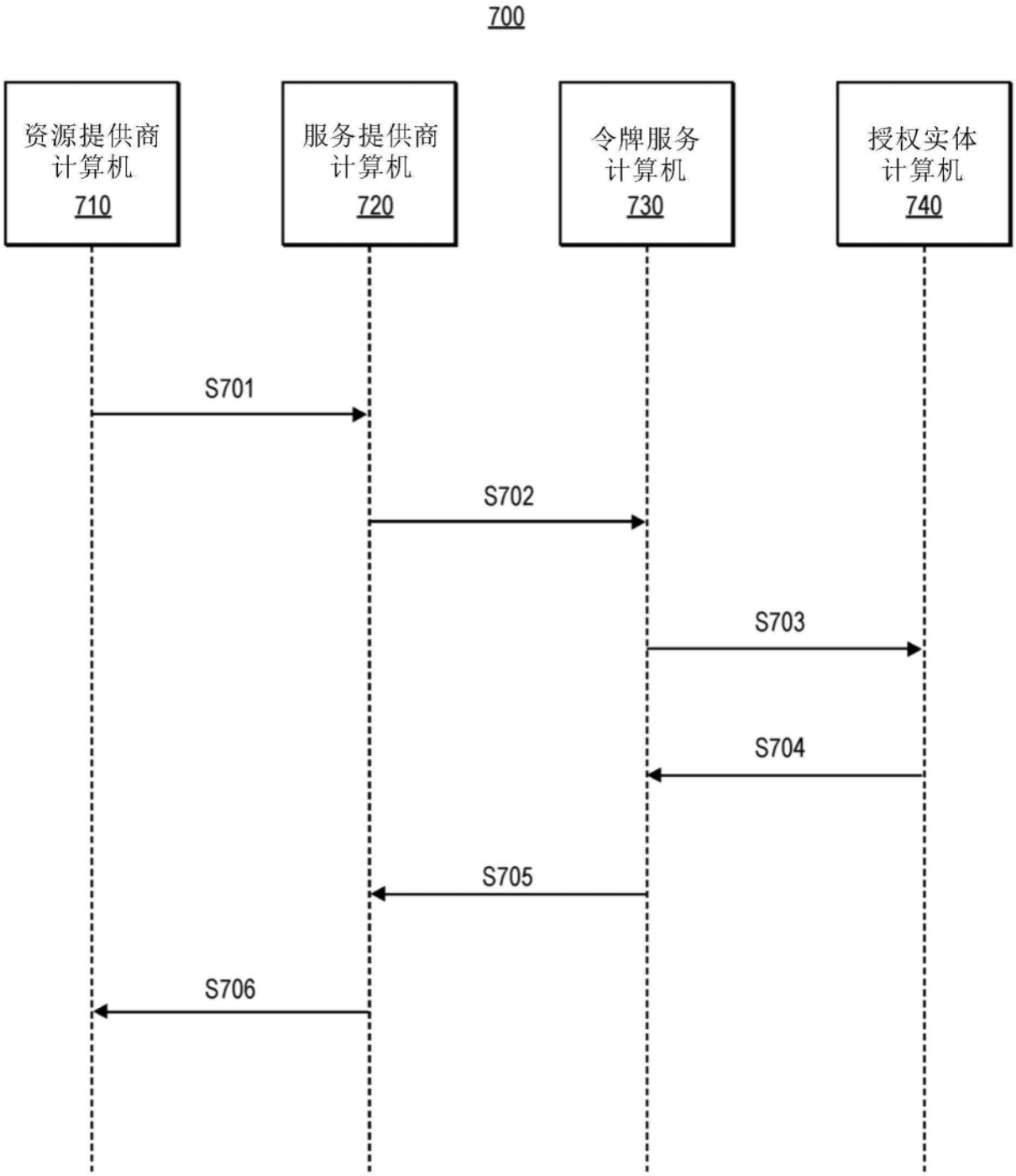

700
资源提供商计算机
710
服务提供商计算机
720
令牌服务计算机
730
授权实体计算机
740
S701
S702
S703
S704
S705
S706

图7

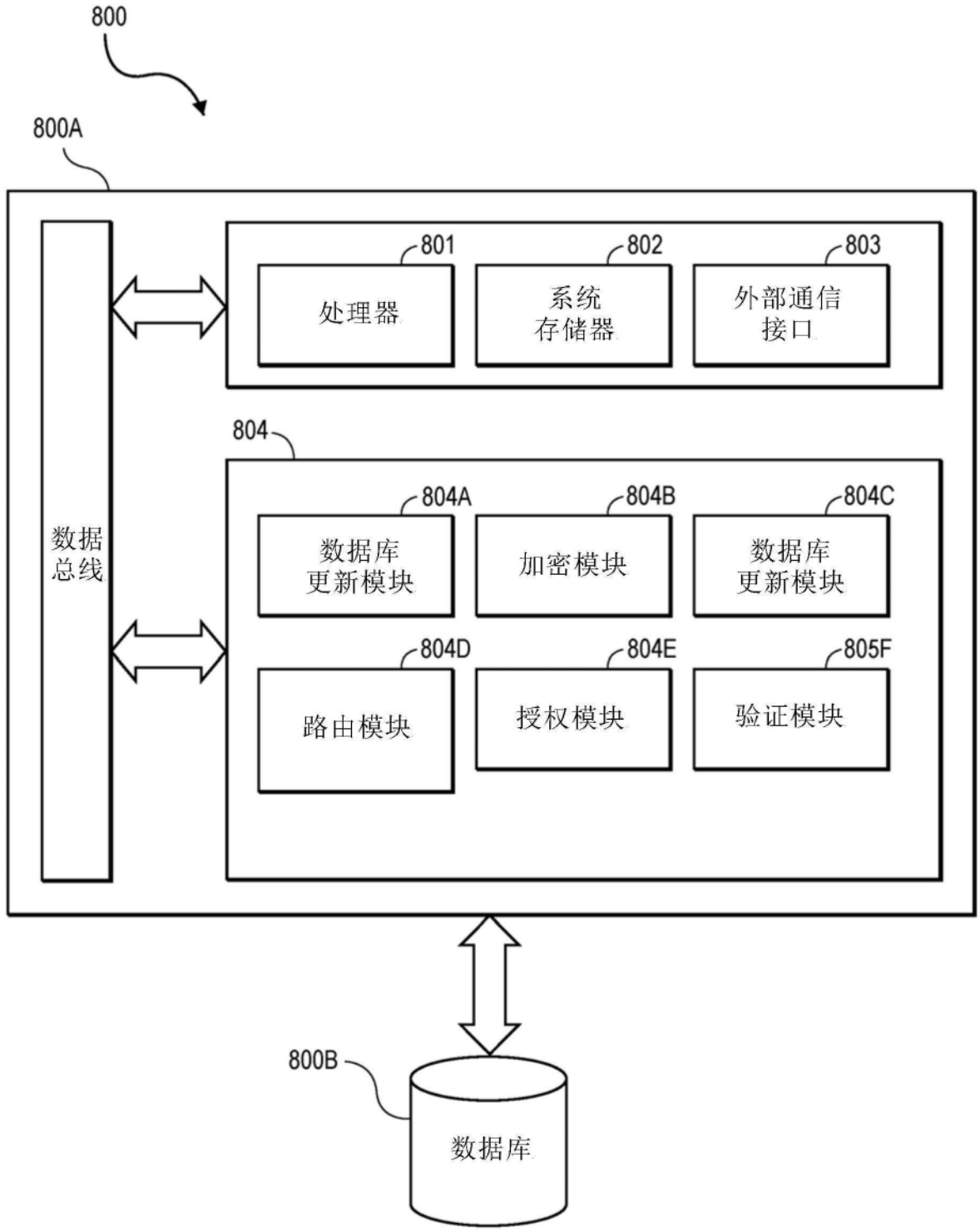

800
800A
801
处理器
802
系统
存储器
803
外部通信
接口
804
804A
数据库
更新模块
804B
加密模块
804C
数据库
更新模块
804D
路由模块
804E
授权模块
805F
验证模块
数据
总线
800B
数据库

图8

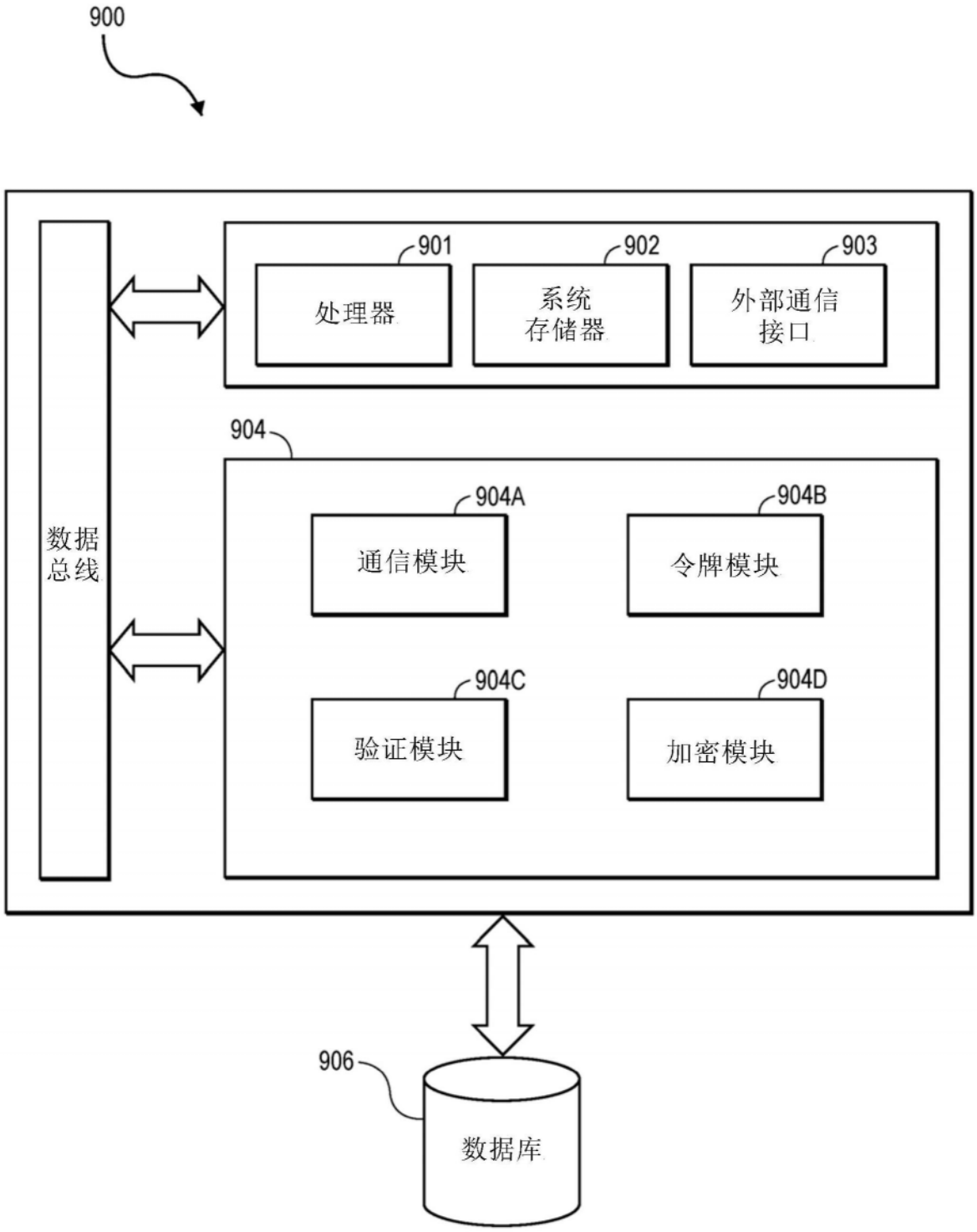

900
901
处理器
902
系统
存储器
903
外部通信
接口
904
904A
通信模块
904B
令牌模块
904C
验证模块
904D
加密模块
数据
总线
906
数据库

图9