(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 105745678 B
(45)授权公告日 2022.09.20

(21)申请号 201480063714.5
(22)申请日 2014.09.22
(65)同一申请的已公布的文献号
申请公布号 CN 105745678 A
(43)申请公布日 2016.07.06
(30)优先权数据
61/880,802 2013.09.20 US
(85)PCT国际申请进入国家阶段日
2016.05.20
(86)PCT国际申请的申请数据
PCT/US2014/056837 2014.09.22
(87)PCT国际申请的公布数据
WO2015/042548 EN 2015.03.26
(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 O·麦克霍顿 K·皮尔扎德
(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 侯颖媛
(51)Int.Cl.
G06Q 20/40(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 1394408 A,2003.01.29
CN 102742211 A,2012.10.17
CN 101563870 A,2009.10.21
US 2011137802 A1,2011.06.09
审查员 王文聪

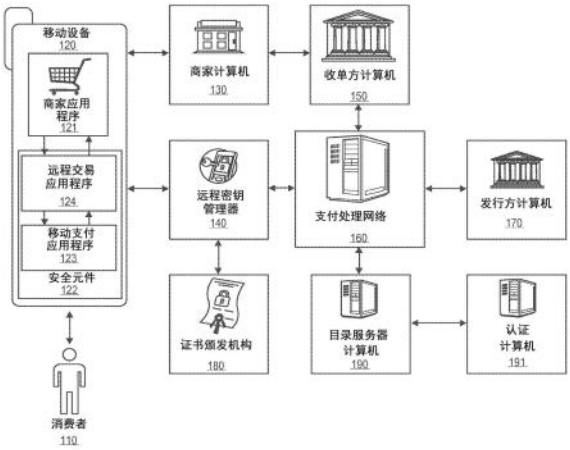
权利要求书3页 说明书36页 附图7页

(54)发明名称

包括消费者认证的安全远程支付交易处理

(57)摘要

本公开涉及包括消费者认证的安全远程支付交易处理。本发明的各实施例涉及用于安全地处理远程交易的方法、设备、计算机可读介质以及系统。一个实施例涉及处理由通信设备发起的远程交易的方法。方法包括服务器计算机接收包括使用第一密钥加密的经加密的支付信息的支付请求。经加密的支付信息包括安全信息。该方法进一步包括使用第二密钥来解密经加密的支付信息，从与发行方相关联的认证计算机获取远程交易的认证响应值，更新经解密的支付信息以包括认证响应值，使用第三密钥来重新加密经解密的支付信息，以及将包括经重新加密的支付信息的支付响应发送到交易处理器。交易处理器使用第四密钥来解密经重新加密的支付信息并使用经解密的支付信息来发起支付交易。



CN 105745678 B

1.一种处理由通信设备发起的远程交易的方法,所述方法包括:

由服务器计算机,从所述通信设备上的移动支付应用程序接收包括经加密的支付信息的支付请求,其中所述经加密的支付信息由所述通信设备上的所述移动支付应用程序通过访问存储在所述通信设备的安全存储器中的支付凭证并且对所述支付凭证加密来生成,所述经加密的支付信息包括安全信息,所述安全信息包括密码和用户认证数据,并且所述经加密的支付信息是使用第一加密密钥加密的;

由所述服务器计算机,使用第二加密密钥来解密所述经加密的支付信息;

由所述服务器计算机,从与账户发行方相关联的认证计算机获取所述远程交易的认证响应值,其中在提供所述认证响应值之前,所述认证计算机验证所述安全信息;

由所述服务器计算机,更新经解密的支付信息以包括所述认证响应值;

由所述服务器计算机,使用第三加密密钥来重新加密所述经解密的支付信息;以及

由所述服务器计算机,将包括经重新加密的支付信息的支付响应发送到与所述通信设备相关联的交易处理器,其中,所述交易处理器使用第四加密密钥来解密所述经重新加密的支付信息并使用经解密的支付信息来发起支付交易,并且所述交易处理器是商家计算机,

其中,获取所述认证响应值进一步包括:

由所述服务器计算机,确定与所述经解密的支付信息相关联的认证计算机;

由所述服务器计算机,将包括所述安全信息的认证请求发送到所述认证计算机;以及

由所述服务器计算机,接收包括所述认证响应值的认证响应,所述认证响应值指出由与所述经解密的支付信息中的账户信息相关联的账户发行方对所述安全信息的验证,

其中验证接收到的所述安全信息包括:

将来自接收到的所述安全信息的所述密码与所述认证计算机生成的密码进行比较;以及

将来自接收到的所述安全信息的所述用户认证数据与存储在认证数据库中的用户认证数据进行比较。

2.如权利要求1所述的方法,其中,所述认证计算机由代表所述账户发行方的支付处理网络操作。

3.如权利要求1所述的方法,其中,所述密码是由所述通信设备的所述移动支付应用程序生成的。

4.如权利要求3所述的方法,其中,所述密码是使用与账户发行方相关联的共享的算法生成的。

5.如权利要求1所述的方法,其中,所述用户认证数据包括由所述通信设备的用户输入的用户数据。

6.如权利要求1所述的方法,其中,所述支付请求消息进一步包括交易处理器证书,所述方法进一步包括使用所述交易处理器通过下列步骤来确定所述第三加密密钥:

验证所述交易处理器证书是可靠的;

利用证书颁发机构确认所述交易处理器证书当前有效;以及

从所述交易处理器证书中提取所述交易处理器公钥。

7.如权利要求1所述的方法,其中,所述交易处理器通过将所述经解密的支付信息映射

到配置成由支付处理网络处理的授权请求消息来发起所述支付交易。

8.如权利要求1所述的方法，其中，由支付处理网络在所述支付交易的发起之后在对所述支付交易的处理期间验证所述认证响应值。

9.如权利要求1所述的方法，其中，所述第一加密密钥包括第三方公钥/私钥对的公钥，其中，所述第三方公钥/私钥对包括第三方公钥和第三方私钥，其中所述第一加密密钥包括所述第三方公钥，且其中所述第二加密密钥包括所述第三方私钥。

10.如权利要求9所述的方法，其中，所述服务器计算机、所述第三方公钥以及所述第三方私钥与支付处理网络相关联。

11.一种服务器计算机，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代码，以用于执行处理由通信设备发起的远程交易的方法，所述方法包括：

从所述通信设备上的移动支付应用程序接收包括经加密的支付信息的支付请求，其中所述经加密的支付信息由所述通信设备上的所述移动支付应用程序通过访问存储在所述通信设备的安全存储器中的支付凭证并且对所述支付凭证加密来生成，所述经加密的支付信息包括安全信息，所述安全信息包括密码和用户认证数据，并且所述经加密的支付信息是使用第一加密密钥加密的；

使用第二加密密钥来解密所述经加密的支付信息；

从与账户发行方相关联的认证计算机获取所述远程交易的认证响应值，其中在提供所述认证响应值之前，所述认证计算机验证所述安全信息；

更新经解密的支付信息以包括所述认证响应值；

使用第三加密密钥来重新加密所述经解密的支付信息；以及

将包括经重新加密的支付信息的支付响应发送到与所述通信设备相关联的交易处理器，其中所述交易处理器使用第四加密密钥来解密所述经重新加密的支付信息并使用所述经解密的支付信息来发起支付交易，并且所述交易处理器是商家计算机，

其中，获取所述认证响应值进一步包括：

由所述服务器计算机，确定与所述经解密的支付信息相关联的认证计算机；

由所述服务器计算机，将包括所述安全信息的认证请求发送到所述认证计算机；以及

由所述服务器计算机，接收包括所述认证响应值的认证响应，所述认证响应值指出由与所述经解密的支付信息中的账户信息相关联的账户发行方对所述安全信息的验证，

其中验证接收到的所述安全信息包括：

将来自接收到的所述安全信息的所述密码与由所述认证计算机生成的密码进行比较；以及

将来自接收到的所述安全信息的所述用户认证数据与存储在认证数据库中的用户认证数据进行比较。

12.如权利要求11所述的服务器计算机，其中，所述密码是由所述通信设备的所述移动支付应用程序生成的。

13.如权利要求11所述的服务器计算机，其中，所述用户认证数据是由所述通信设备的用户输入的用户数据。

14.如权利要求11所述的服务器计算机，其中，由支付处理网络在所述支付交易的发起之后在对所述支付交易的处理期间验证所述认证响应值。

15.一种用于处理远程交易的系统，所述系统包括：

如权利要求11所述的服务器计算机；

所述通信设备，所述通信设备配置成将包括安全信息的支付请求发送到所述服务器计算机；以及

所述认证计算机，所述认证计算机配置成从所述服务器计算机接收认证请求，验证所述安全信息，生成包括所述认证响应值的认证响应，以及将所述认证响应发送到所述服务器计算机。

包括消费者认证的安全远程支付交易处理

[0001] 相关申请的交叉引用

[0002] 本申请是2013年9月20日提交的美国临时申请No.61/880,802的非临时申请并要求其优先权的权益,出于所有目的,该申请通过整体引用结合于此。本申请涉及2014年7月15日提交的美国非临时申请No.14/332,245,以及2014年8月15日提交的美国非临时申请No.14/461,227,出于所有目的,这两项申请通过引用整体结合在此。

技术领域

[0003] 本公开涉及支付交易处理,尤其涉及安全远程支付交易处理。

背景技术

[0004] 传统的远程交易具有有限的安全特征以及较高的诈骗风险,因为消费者通常不在商家处或服务提供商处以便确认支付凭证未被盗取或被截取并且未被恶意的第三方使用。相应地,需要提高从通信设备发起的远程交易的安全性。

[0005] 另外,使用通信设备(例如,移动设备)上的不受信任的商家应用程序来执行远程支付可能会导致严重的数据安全性问题,因为难以判断应用程序是否是恶意软件或以别的方式试图窃取敏感信息。相应地,需要一种安全远程交易处理系统,该安全远程交易处理系统在远程交易过程中以有效率且安全的过程来认证设备以及与设备相关联的用户以便敏感信息可以受到保护而免受恶意或不受信任的应用程序的影响。

[0006] 另外,虽然实现基于安全元件的远程支付交易的系统可以提供设备认证和验证,但是这些系统无法在认证过程期间认证与发起支付交易的通信设备相关联的消费者或用户。相应地,被窃取和/或破解的设备仍可能用于执行诈骗交易,并且系统资源可用于处理诈骗交易并针对用户、设备等执行多个单独的认证过程。因此,需要一种以高效率的方式提供用户和设备认证的认证过程。

[0007] 进一步地,允许通过用户名和密码认证或质询-响应认证来认证用户的传统的电子商务交易系统无法为账户发行方或服务提供商提供对远程交易的认证过程或授权过程的直接控制。因此,与在远程交易中使用的账户相关联的发行方可能不能被给予账户发行方及其他服务提供商可能期望的控制和风险分析的等级。因此,需要一种允许由与远程交易相关联的发行方对认证过程进行直接控制的系统。

[0008] 本发明的各实施例单独地且共同地解决这些问题以及其他问题。

发明内容

[0009] 本发明的各实施例涉及用于安全地处理使用通信设备的包括消费者认证的远程交易的方法、设备、计算机可读介质和系统。例如,本发明的各实施例允许消费者使用包括安全且敏感的支付凭证的移动设备发起并处理通过商家网站或商家应用程序发起的远程支付交易。商家网站或商家应用程序可以利用基于安全元件的移动支付应用程序来从通信设备中获取支付凭证(例如,帐号和到期日期),而不是让消费者使用小键盘提供帐号和到

期日期或从不安全的存储器获取该信息。因此，各实施例提供了一种安全过程，用于传输敏感的支付信息以及认证用户和支付应用程序，同时保护敏感信息免遭不受信任的、不不安全的和/或可能恶意的移动应用程序(例如，商家应用程序)的影响。

[0010] 进一步，各实施例包括针对通过通信设备的支付应用程序发起的远程交易而使用包括用于认证设备的基于芯片的安全值(例如，密码)以及用于认证用户的用户认证数据(例如，个人标识号(PIN)、密码、口令(passcode)等等)的安全信息。因此，各实施例在传统的电子商务或远程支付交易上提供附加的安全性。因此，各实施例提供更安全的且稳健的远程支付交易系统。如此，各实施例通过在通常不具有包含这种安全特征的能力的交易中提供可确认的安全信息，增强了“无卡”交易的安全级别。

[0011] 本发明的一个实施例涉及处理由移动设备发起的远程交易的方法。该方法包括服务器计算机接收包括经加密的支付信息的支付请求。经加密的支付信息包括安全信息，并且是使用第一加密密钥加密的。该方法进一步包括使用第二加密密钥来解密经加密的支付信息，以及从与账户发行方相关联的认证计算机获取远程交易的认证响应值。在向服务器计算机提供认证响应值之前，认证计算机验证安全信息。该方法进一步包括服务器计算机更新经解密的支付信息以包括认证响应值，使用第三加密密钥来重新加密经解密的支付信息，以及，将包括经重新加密的支付信息的支付响应发送到与通信设备相关联的交易处理器。交易处理器使用第四加密密钥来解密经重新加密的支付信息，并使用经解密的支付信息来发起支付交易。

[0012] 本发明的另一实施例涉及服务器计算机，该服务器计算机包括：处理器以及耦合到该处理器的计算机可读介质。计算机可读介质包括可由处理器执行的用于执行处理远程交易的方法的代码。处理远程交易的方法包括服务器计算机接收包括经加密的支付信息的支付请求。经加密的支付信息包括安全信息并且使用第一加密密钥加密。该方法进一步包括使用第二加密密钥来解密经加密的支付信息以及从与账户发行方相关联的认证计算机获取远程交易的认证响应值。在向服务器计算机提供认证响应值之前，认证计算机验证安全信息。该方法进一步包括服务器计算机更新经解密的支付信息以包括认证响应值，使用第三加密密钥来重新加密经解密的支付信息，以及将包括经重新加密的支付信息的支付响应发送到与通信设备相关联的交易处理器。交易处理器使用第四加密密钥来解密经重新加密的支付信息，并使用经解密的支付信息来发起支付交易。

[0013] 本发明的另一实施例涉及用于处理远程交易的系统。系统包括配置成将包括经加密的支付信息的支付请求发送到服务器计算机的通信设备。经加密的支付信息包括安全信息，并且经加密的支付信息使用第一加密密钥加密。系统进一步包括配置成接收包括经加密的支付信息的支付请求的服务器计算机。该服务器计算机进一步配置成使用第二加密密钥来解密经加密的支付信息，以及从与账户发行方相关联的认证计算机获取远程交易的认证响应值。该服务器计算机进一步配置成更新经解密的支付信息以包括认证响应值，使用第三加密密钥来重新加密经解密的支付信息，以及将包括经重新加密的支付信息的支付响应发送到与通信设备相关联的交易处理器。交易处理器配置成使用第四加密密钥来解密经重新加密的支付信息，并使用经解密的支付信息来发起支付交易。系统进一步包括认证计算机，所述认证计算机配置成从所述服务器计算机接收包括安全信息的认证请求，验证所述安全信息，生成包括认证响应值的认证响应，以及将所述认证响应发送到所述服务器计

算机。

[0014] 下面更详细地描述了本发明的这些及其他实施例。

附图说明

[0015] 图1示出了根据本发明的一些实施例的用于使用与支付处理网络相关联的远程密钥管理器和移动设备的商家应用程序来执行远程交易的示例性系统的框图。

[0016] 图2示出了可以与本发明的一些实施例一起使用的示例性移动设备的框图。

[0017] 图3示出了根据本发明的一些实施例的配置成管理远程交易的双因素认证的示例性远程密钥管理器的框图。

[0018] 图4示出了根据本发明的一些实施例的配置成管理远程交易的认证请求和响应并处理安全的远程交易的示例性支付处理网络的某些部件的框图。

[0019] 图5示出了根据本发明的一些实施例的用于使用证书颁发机构来供应商家公钥/私钥对和商家应用程序证书的示例性方法的流程图。

[0020] 图6示出了根据本发明的一些实施例的用于使用远程密钥管理器、支付处理网络以及移动设备的商家应用程序来处理远程交易的示例性方法的流程图。

[0021] 图7示出了示例性计算机设备的框图。

具体实施方式

[0022] 本发明的各实施例涉及用于安全地处理由通信设备上的不受信任的商家应用程序发起的远程交易的系统和方法。不受信任的应用程序可能是合法的应用程序，但是由于应用程序运行的不安全的或可能不安全的环境，该应用程序可能不会被存储或控制对用于交易(或多个交易)的敏感信息的访问的安全应用程序或受信任的执行环境信任。各实施例提供一种安全系统，该安全系统保护存储在移动设备的安全存储器中的敏感的支付信息，在提供敏感信息之前验证商家应用程序，以安全且有效率的方式认证与所述远程交易相关联的用户和设备两者，以及允许敏感的支付信息以安全的方式传输以使用通信设备来执行远程支付交易。

[0023] 当在通信设备上执行远程电子商务交易(即e商务)时，消费者向商家网站或web服务器提供支付凭证以及其他敏感信息，以便商家可以标识并发起对于交易的支付。通常，消费者可以向移动设备键入或以别的方式输入主要账户号码(PAN)、到期日期，以及卡确认值(例如，CVV2)，然后移动设备将该信息发送到商家服务器。然而，此方法不安全，并可能会导致欺骗性的交易。例如，在没有适当的授权的情况下，商家没有办法知道消费者是否是可靠的或消费者是否拥有基础支付设备或消费者是否获取了PAN、到期日期以及卡确认值。

[0024] 本发明的各实施例通过单一接口系统在通信设备(例如，移动设备)和认证服务器之间提供端对端安全认证过程以用于处理远程交易。与账户发行方相关联的认证计算机可以通过安全且有效率的通信架构，直接从通信设备接收认证数据，验证认证数据，以及授权与远程交易相关联的请求的交易(或其他操作)。进一步地，认证数据可通过在单一通信和认证过程中包括设备(例如，使用共享的秘密生成的安全值)和用户认证数据(例如，个人标识号、口令，等等)两者而包括两个因素认证。

[0025] 因此，各实施例在发起远程交易之前，允许认证与设备相关联的安全值和与用户

相关联的用户认证数据，以及向支付处理网络和/或账户发行方提交其他支付数据以供确认。在通过支付处理网络发起远程交易之前，可以由认证计算机提供认证响应，并且认证响应值可以嵌入到支付数据中以用于处理交易。因此，在交易处理过程中，可以由支付处理器和/或发行方验证认证响应值，作为用于远程交易处理的增加的安全措施。

[0026] 根据本发明的各实施例，商家web服务器计算机或商家应用程序可以从安全地存储了账户信息的通信设备的移动支付应用程序安全地获取账户信息。另外，因为使用可以配置成连同支付凭据一起提供安全信息的支付应用程序来处理交易，所以远程交易可在远程交易过程中包括较高安全性的动态的基于芯片的安全数据(例如，动态密码)。相应地，在电子商务交易期间，其中由于消费者键入账户信息和/或缺乏对嵌入在智能卡或移动设备中的安全芯片的访问，商家通常将不能接收高度安全的基于芯片的安全数据，本发明的各实施例提供动态认证信息以及其他芯片数据以用于在交易处理过程中验证。

[0027] 进一步地，各实施例允许商家计算机在远程支付交易过程中从支付应用程序安全地接收账户凭证、用户认证数据，以及设备安全性信息。相应地，远程商家服务器计算机可以接收足够的数据以构建“卡存在”芯片交易授权请求消息，这比典型的远程交易提供更高级别的安全性。

[0028] 本发明的各实施例具有多个优点。例如，各实施例改善了使用移动设备上的不受信任的或未知的商家应用程序的支付交易的安全性。在一些实施例中，可以使用远程密钥管理器、移动网关、支付处理网络、移动钱包提供商，或任何其他第三方系统来验证与商家证书相关联的商家应用程序，确定与经验证的商家应用程序相关联的商家密钥，解密支付信息，以及使用受信任的商家的公钥来重新加密支付信息。这防止了未经授权的应用程序或设备访问敏感数据，因为在没有受信任的交易处理器加密密钥(例如，商家私钥、商家应用程序私钥、收单方私钥，等等)的情况下，支付信息是不可读取的。

[0029] 进一步地，各实施例在远程交易过程中且在发起远程交易之前，通过对用户和设备(例如，支付应用程序)的双因素认证，进一步改善了在不安全的通信设备环境中发起的远程支付交易的安全性。

[0030] 进一步，由于远程交易处理中涉及的多个密钥交换，敏感信息可以在被传输或传递到目的地实体时始终被保护。相应地，各实施例提供用于传输与远程交易相关的敏感信息的安全通信过程，以允许保护敏感信息，敏感信息可能是静态的并且可在未来的交易中重复使用(例如，静态账户标识符、到期日期，等等)。

[0031] 另外，各实施例提供比包括单独的认证过程的系统提供执行用户和设备认证两者的更有效率的方法。例如，允许用户被账户发行方或支付处理器认证的传统的远程交易认证系统在电子商务交易过程中要求用户通过单独的或并行的过程验证他们的身份。例如，消费者可以登录到在线账户，并与他们的支付凭证一起提交密码。这对于认证系统是效率低的并且对于消费者是累赘的。相比之下，本发明的各实施例允许以容易且有效率的方式进行用户和设备认证。

[0032] 进一步地，各实施例在通信设备和发行方系统之间要求较少的集成，因为各实施例为通信设备提供单点联系，而不是像先前的系统可能要求通信设备的重新定向到与不同的账户发行方相关联的每一个访问控制服务器或认证服务器。相应地，本发明的各实施例提供与远程密钥管理器的单个安全的集成点的优点，然后，该远程密钥管理器可以利用认

证计算机认证远程交易并将认证结果直接返回到通信设备。

[0033] 因此，系统避免使用对于每一发行方或服务提供商将通信设备定向到认证计算机的重新定向方案。对于多种认证计算机的重新定向引发许多集成问题，其中，与不同的发行方或其他服务提供商相关联的每一特定认证计算机都具有不同的通信协议、安全性置换、接口命令组，等等。因此，在本发明的各实施例中，通信设备的移动支付应用程序和/或远程交易应用程序可以实现单组API或其他命令来发起认证过程。因此，通信设备与远程密钥管理器的集成更加容易地管理，并且对远程交易应用程序要求较少的更新、改变以及修改。

[0034] 因此，本发明的各实施例提供一种安全远程交易处理系统，该远程交易处理系统允许(1)在提供敏感信息之前确认不受信任的或未知的商家应用程序，以及，(2)提供将信息传输到单一集成点的安全通信方案，以便在通过支付处理网络发起交易之前，对(i)消费者以及(ii)设备进行验证和认证。因此，各实施例提供执行安全远程支付交易的更有效率的安全的且容易实现的方法，包括通过单一认证过程来认证消费者。

[0035] 另外，各实施例还通过允许在交易过程中使用高度安全的且难以再生的信息来提供更安全的支付系统。例如，在交易过程中提供的动态密码或动态值允许商家较高级别地相信消费者事实上被授权使用该账户执行交易。因此，支付处理网络、发行方以及商家将处理较少的欺骗性交易和拒绝付款。

[0036] 最后，各实施例对消费者和用户更方便，因为系统允许消费者使用已经存在于移动设备上的支付信息(例如，账户信息)来发起并处理交易。以前的远程交易要求消费者手动输入支付信息或使用不存储在安全存储器中的信息。因此，各实施例为消费者从移动设备发起交易提供更安全且方便的方法。

[0037] 在讨论本发明的各实施例之前，对某些术语的描述可能会对理解本发明的各实施例有帮助。

[0038] “远程交易”可包括交易一方与交易另一方相隔某距离和/或被设备隔开的任何交易。例如，远程交易可包括经由两个或多个设备之间的通信执行的“无卡交易”、电子商务或其他线上交易。例如，远程交易可包括不在相同位置的设备或双方(例如，商家和消费者)不使用相同的设备来完成交易情况下的多个设备。另外，远程交易可包括不使用商家销售点设备(即，访问设备)完成的而是由消费者使用他们的移动设备与配置成处理远程交易的远程(或本地)商家服务器计算机进行通信来完成的店内交易。传统上，远程交易具有较高的欺骗可能性，因为远程交易不允许收款人有机会标识付款人或以别的方式确保他们正在接收的支付是合法的，因为在交易过程中双方不在相同的位置(诸如在“卡存在”或店内交易中)。本地、有卡、面对面或店内交易可包括一种交易，在该交易中，双方或多方交易处于同一地点，使用相同的交易设备或者通过指示一个存在的个人或实体认证付款方和/或收款方的身份来执行。

[0039] 另外，远程交易还可包括任何类型的交易。例如，远程交易可包括支付交易(例如，与商品或服务与货币值的交换相关联的交易)，非支付交易(例如，认证交易、账户供应交易，或不涉及货币值与商品或服务的交换的任何其他交易)，和/或与通信设备、移动应用程序、支付应用程序、支付处理网络、发行方和/或交易处理系统内的任何其他实体相关联的任何其他类型的交易。

[0040] “支付请求”可包括包含处理或发起支付的请求的消息。例如，可以从与消费者相

关联的移动设备发送关于与由商家所提供的商品或服务相关联的购买交易的支付请求。支付请求可包括与交易相关的任何信息，包括支付信息(例如，账户标识符、个人信息，等等)、交易信息(例如，商家信息、正在被购买的商品，等等)、设备信息(例如，移动设备电话号码、安全元件标识符，等等)、路由信息(例如，目的地计算机的因特网协议(IP)地址、目的地计算机的标识符、银行标识号码(BIN)，等等)，以及与支付交易相关的任何其他信息。例如，支付请求可包括交易的经加密的支付信息，并且可以被发送到第三方计算机，该第三方计算机配置成认证支付请求、验证公钥证书、解密经加密的支付信息、从经验证的证书中提取公钥，重新加密经解密的支付信息，以及将经重新加密的支付信息发送到交易处理器，以便发起支付交易。相应地，支付请求可包括与用于将敏感数据传输到用于处理远程交易的商家服务器的安全过程相关的任何信息。

[0041] “支付信息”可包括用于执行支付的任何相关信息。例如，支付信息可包括可以被用来在发行方处标识和/或认证消费者账户的任何敏感的账户信息和/或个人信息。进一步，在一些实施例中，支付信息也可以包括商家信息、消费者信息、移动设备信息、路由信息，或可以被用来支配、管理并传递支付交易的任何其他相关信息。如此，支付信息可包括敏感的信息以及不敏感的信息两者。另外，支付信息还可包括可以被用来执行交易的账户信息、个人信息等的一部分。例如，支付信息可包括与交易或账户相关联的敏感信息，并可以与可能不被视为支付信息的其他不敏感信息(例如，交易金额，等等)一起发送。

[0042] “支付凭证”可包括允许处理器标识、确认和/或处理使用消费者账户的支付交易的任何信息。例如，支付凭证可包括账户标识符(例如，主账户号码(PAN))、令牌(例如，账户标识符替代物)、到期日期、卡确认值(例如，CVV、CVV2、dCVV，等等)、动态密码或动态值(例如，动态认证数据)、与账户相关联的个人信息(例如，地址等等)、账户别名，或任何其他相关信息。

[0043] 在一些实施例中，支付凭证可以存储在移动设备的安全存储器中。移动设备的安全存储器可以被配置为使得存储在安全存储器中的数据可不被外面的应用程序直接访问以及可以访问与安全存储器相关联的移动支付应用程序来获取存储在安全存储器上的支付凭证。相应地，商家应用程序可以与移动支付应用程序或与远程交易应用程序或其他应用程序连接，以便与移动支付应用程序连接，以便访问存储在安全存储器上的支付凭证。在一些实施例中，可以访问软件开发工具包(SDK)、应用程序编程接口(API)，或其他第三方编程代码或模块，以便从移动支付应用程序请求支付凭证。进一步，在一些实施例中，安全存储器可以被配置为使得可以基于与存储在移动设备的安全存储器上的支付凭证的发行方相关联的共享的主衍生密钥(MDK)来使用会话衍生密钥而以加密的形式提供支付凭证或任何其他支付信息。另外，还可以存在有效数字或公钥证书，以供应用程序、SDK或API访问安全存储器(例如，安全元件)。

[0044] “交易信息”可包括与交易相关联的任何数据。例如，交易信息可包括交易金额、交易时间、交易日期、商家信息(例如，注册的商家标识符、地址、商家计算机IP地址，等等)、产品信息(例如，序列号、产品名称或其他标识符，等等)。可以在消费者通过商家应用程序发起支付交易之前或之后，由商家服务器计算机向通信设备(例如，移动设备)提供交易信息。在一些实施例中，可使用交易信息以使用交易信息中所包括的商家信息来标识与交易相关联的特定的商家。

[0045] “商家信息”可包括与商家、收款人、服务提供商、生产者，或交易中的其他依赖方相关联的任何信息。例如，商家信息可包括在向远程支付服务、远程密钥管理器、支付处理网络、或与远程交易处理系统相关联的其他交易处理实体注册的过程中确定的商家标识符。在一些实施例中，商家标识符可以被用来确定与交易相关联的注册的商家计算机公钥、商家应用程序公钥，和/或收单方公钥。

[0046] “经加密的支付信息”可包括对于某方难以理解以防止对支付信息的未经授权的访问的任何支付信息。例如，没有获取共享秘密(shared secret)或没有获取指定的加密密钥的接收方不可读取加密的支付信息。如此，可以通过可逆的且可重复的过程使经加密的支付信息难以理解，从而两个实体可以使用共享秘密或加密密钥共享信息，而未经授权的实体不能够理解或访问敏感的支付信息或支付信息内的敏感的支付凭证(除非他们能够访问共享秘密或加密密钥)。

[0047] 另外，在一些实施例中，经加密的支付信息可包括经加密的敏感信息和未加密的较不敏感的或非安全信息的任何组合。例如，在一些实施例中，经加密的支付信息可包括经加密的支付凭证(例如，敏感的账户标识符和到期日期)和未加密的交易信息(例如，交易金额、产品标识符，等等)。在其他实施例中，经加密的支付信息可包括经加密的全部相关交易信息。例如，在一些实施例中，经加密的支付信息可包括经加密的支付凭证和经加密的交易信息两者。

[0048] 在一些实施例中，经加密的支付信息可以由移动设备的移动支付应用程序生成，以便移动支付应用程序可以具有用于加密存储的或接收到的支付凭证和/或用于交易的其他支付信息的加密密钥(例如，第三方公钥)。例如，移动支付应用程序可以存储第三方公钥。第三方公钥可以与可以安全地存储在远程密钥管理器、移动网关、支付处理网络、移动钱包提供商，或被配置成处理远程支付交易的任何其他第三方上的第三方私有的加密密钥配对。第三方私钥可以被用来解密经加密的支付信息并允许第三方进一步利用指定的交易处理器的公钥来加密安全支付信息。相应地，经加密的支付信息可以被用来允许安全的远程交易处理。另外，第三方加密密钥可包括对称的加密密钥，密钥不限于公钥/私钥对。

[0049] “经解密的支付信息”可包括从难以理解的状态转换到可理解的状态的支付信息。例如，经解密的支付信息可包括对经加密的支付信息应用合适的加密密钥以获取原始支付信息的结果。例如，可以将第三方私钥应用于利用第三方公钥加密的经加密的支付信息，以便解密经加密的支付信息并获取底层支付信息。进一步，在经加密的支付信息包括经加密的和未加密的信息两者的情况下，可以通过解密经加密的部分而不解密未加密的部分来获取经解密的支付信息。

[0050] “经重新加密的支付信息”可包括在至少被解密一次之后又已经被弄得难以理解以防止对支付信息的未经授权的访问的任何支付信息。例如，经重新加密的支付信息可以使用与最初加密的支付信息不同的加密密钥或加密算法来加密或以别的方式使其无法被未经授权的实体理解。例如，分别使用第三方公钥和私钥(或第三方对称加密密钥)加密和解密的经解密的支付信息，可以使用交易处理器公钥(例如，商家公钥、商家应用程序公钥、收单方公钥，等等)重新加密并发送到交易处理器。如此，相同信息(例如，支付信息)可以使用允许两个不同的实体安全地获取底层信息而同时防止信息被任何其他实体访问的两个不同的密钥来加密。

[0051] “支付响应”可包括包含对请求的响应以处理或发起支付的消息。例如，可以响应于与远程交易请求(远程交易请求与由商家所提供的商品或服务相关联)相关联的购物请求，从服务器计算机发送支付响应。支付响应可包括与交易相关的任何信息，包括支付信息(例如，账户标识符、个人信息，等等)、交易信息(例如，正在被购买的商品，商家信息、等等)、设备信息(例如，移动设备电话号码、安全元件标识符，等等)、路由信息(例如，目的地计算机的因特网协议(IP)地址、目的地计算机的标识符、银行标识号码(BIN)，等等)，以及与支付交易相关的任何其他信息。例如，支付响应可包括利用交易处理器公钥加密的经重新加密的支付信息，并可以将其发送到交易处理器，供进一步处理。例如，交易处理器可以使用交易处理器私钥，解密经重新加密的支付信息，并可以使用经解密的支付信息，发起支付交易。进一步，在一些实施例中，支付响应可包括标识交易、账户、消费者，和/或交易的其他实体是否被认证的认证响应信息。

[0052] “移动网关”可以是被配置成与通信设备进行通信的服务器计算机或服务器计算机系列。例如，移动网关可以使用无线电(OTA)消息或使用任何其他通信网络和协议，与移动设备进行通信。例如，移动网关可以被配置成提供与移动设备安全通信的信道(即，安全信道)，通过该安全信道，可以使用移动通信网络、因特网，和/或任何其他相关通信网络，将信息安全地传输到移动设备以及从移动设备安全地发送信息。

[0053] “交易处理器”可包括与处理交易相关联的任何实体。例如，商家、通信设备(例如，移动设备、台式计算机，等等)，商家应用程序或通信设备上的其他移动应用程序(例如，收单方应用程序或支付服务提供商应用程序)、收单方计算机、支付处理网络，以及交易处理生态系统中的任何其他实体都可以是交易处理器。在一些实施例中，交易处理器可以与在对远程支付交易的处理过程中可以被用来加密和解密支付信息的特定公钥(例如，商家公钥、商家应用程序公钥、收单方公钥，等等)和私钥(例如，商家私钥、商家应用程序私钥、收单方私钥，等等)相关联。

[0054] 如此，在一些实施例中，交易处理器可包括被配置成解密经加密的(或经重新加密的)支付信息并发起支付交易的任何实体。可以通过任何合适的方式，发起支付交易，包括将经解密的支付信息传递到另一方，或通过生成经解密的支付信息和/或将其映射到授权请求消息。例如，在一些实施例中，交易处理器可以通过将经解密的支付信息映射到被配置成由支付处理网络处理的授权请求消息，发起支付交易。

[0055] “安全信息”可包括可以被用来认证或验证某一方或设备的任何数据。例如，安全信息可包括用户认证数据，以便认证设备的用户、账户持有人，或与账户或交易相关联的消费者。另外，安全信息可包括与设备、账户或账户发行方相关联的安全值。

[0056] “用户认证数据”可包括可以被用来验证用户的身份或权限的任何信息。例如，用户认证数据可包括个人标识号(PIN)、口令、密码、用户名，或在受信任的各方之间共享的任何其他秘密信息，以便验证一方或多方的身份。例如，在一些实施例中，用户认证数据可包括个人标识号(PIN)、口令、密码、生物测定标识符中的一个或多个，或可以被另一方共享和验证的任何其他唯一用户信息。另外，用户认证数据还可包括以前认证的用户的指示(例如，用户的生物测定验证的结果)。

[0057] 另外，安全信息还可包括可以被用来认证设备的安全值。“安全值”可包括可以被用来将设备、账户，或支付应用程序认证为是可靠的的任何信息。安全值可包括静态值或动

态值。进一步，可以使用共享秘密或其他算法生成安全值，该安全值可以由另一实体或系统验证。例如，安全值可包括可以随着时间而变化(例如，周期性地)、每次使用变化(例如，每次交易)，和/或基于接收到的信息(例如，向算法的输入信息)而变化的动态值，并可以由也可以访问共享的算法和输入数据以重新创建并验证安全值的系统验证。例如，每当交易被发起时，安全值都可以变化并可以使用在两个实体之间共享的秘密算法或其他共享的信息来生成，以使得一个实体可以验证其他实体可以访问共享的秘密从而验证该其他实体可靠的。这也可以被称为“认证数据”。

[0058] 在一些实施例中，安全值可包括密码。例如，可以基于消费者设备和/或发行方账户特定的衍生算法在每次交易时都生成密码，并可以针对每一次交易在支付处理器或账户的发行方出验证该密码。这样的动态值可以被称为动态卡确认值(例如，dCVV、dCVV2)、唯一认证确认值(UAVV)、令牌认证确认值(TAVV)，等等，并可以基于输入数据和用于生成可验证的动态值的算法来区别它们。例如，令牌认证确认值可以使用令牌(或其他账户替代物)作为对确认算法的输入，而动态卡确认值可以使用主账户号码(PAN)作为对相同或不同的确认算法的输入。

[0059] 在其他实施例中，用于生成安全值的秘密算法可以被单一实体知道。例如，在一些实施例中，可以在生成授权请求消息之前认证远程交易并且发行方或支付处理网络可以使用秘密算法来生成认证响应值。当发起交易并生成授权请求消息时，认证响应值可以被包括在授权请求消息中，支付处理网络或账户发行方可以使用相同的秘密算法和输入数据来验证认证响应值，从而验证交易。相应地，安全值可包括使用共享的密钥(例如，动态确认值、令牌认证数据，等等)或秘密密钥(例如，认证响应值)生成的密码。

[0060] 在一些实施例中，支付处理网络和/或发行方计算机170可以在接收对于支付交易的授权请求消息之前，认证安全信息。在这样的实施例中，支付处理网络和/或发行方计算机可以返回认证响应，包括指出对认证信息的验证的认证信息是否被认证和/或验证的认证响应值。相应地，远程交易处理器(例如，支付处理网络计算机、移动网关、远程密钥管理器计算机，等等)可以在重新加密支付信息并发送到交易处理器以便发起支付交易之前，利用支付信息中的认证响应值来替换认证信息。此后，可以将认证响应值返回到支付处理网络，以便通知交易实体，支付交易预先被认证。这样的系统提高了交易处理系统的安全，并最小化交易是诈骗的机率，因为在在交易处理过程中的各种时间发生多个认证过程。另外，这样的系统还可以在通过支付处理网络并通过单一认证过程提交交易之前，有效率地认证用户和支付设备。

[0061] “认证响应值”可包括通知实体数据、实体或过程被认证的任何数据。例如，可以类似于上文说明的安全值，生成认证响应值，但是，也可以使用不同的共享的秘密或算法来生成它，以便交易处理生态系统内的可以访问共享的秘密的另一实体可以判断，消息，账户，或消息中所包括的其他信息被实体认证。例如，与交易相关联的特定静态数据元素(账户标识符、到期日期、交易时间，日期，等等)可以被用作输入，以在认证过程中生成认证响应值，并可以在接收到授权请求消息之后，在支付阶段，重复计算(使用相同数据元素)，以验证认证响应值是正确的并与相同交易信息相关联。

[0062] “支付应用程序”或“移动支付应用程序”可包括被配置成促进来自通信设备(例如，移动设备或任何其他电子通信设备)的支付交易的任何应用程序。例如，移动支付应用

程序可以以安全的方式存储消费者账户的敏感的支付信息和/或支付凭证，以使得支付信息、账户信息、支付凭证、个人信息或任何其他相关信息可以受到保护而免受未经授权的访问。支付应用程序可以被配置成将敏感信息提供到通信设备上的经授权的软件应用程序或模块，免接触元件，或被配置并被授权与支付应用程序进行通信的任何其他软件或硬件。例如，移动支付应用程序可以被配置成与移动设备上的其他移动应用程序或商家应用程序连接，以便提供交易的支付信息。例如，移动支付应用程序可以提供商家应用程序和/或其他移动应用程序可以用来与移动支付应用程序连接的软件开发工具包(SDK)或应用程序编程接口(API)。移动支付应用程序可以被配置成使用安全存储器上的存储的密钥，以加密形式，提供敏感信息。

[0063] 进一步，在一些实施例中，移动支付应用程序可以包括任何API、服务、应用程序、小程序，或适合于从安全元件中检索信息，生成交易的支付信息(例如，密码或其他安全值，经加密的支付凭证，等等)，并与远程交易应用程序，商家应用程序，和/或任何其他应用程序进行通信以便安全地与服务器计算机(例如，远程密钥管理器、移动网关、支付处理网络、第三方服务提供商，等等)进行通信的其他可执行代码。移动支付应用程序可包括或被配置成获取存储的信息，包括支付处理网络公钥、支付凭证、第三方密钥、移动网关凭证，和/或任何其他相关信息，并可以能够与移动网关或其他远程服务器计算机进行通信，以获取任何相关信息的发行方更新。

[0064] “商家应用程序”或“移动应用程序”可包括与交易的一方相关联的任何应用程序。例如，商家应用程序可以与特定商家相关联或可以与许多不同的商家相关联，并可以能够标识是交易的各方的特定商家(或多个商家)。例如，商家应用程序可以存储标识配置成提供销售环境的特定商家服务器计算机的信息，在该销售环境中，商家服务器计算机能够处理由商家应用程序发起的远程交易。进一步，商家应用程序也可以包括通用浏览器或被设计用于与多个商家服务器计算机进行交互的其他软件，只要浏览器被配置成标识商家服务器计算机并处理远程交易。商家应用程序可以安装在移动设备的通用存储器上，如此，可能容易受到恶意攻击、崩溃等等。相应地，商家应用程序可以被移动设备和远程支付交易处理系统内的安全系统视为不受信任的或未知应用程序。

[0065] 在一些实施例中，商家应用程序可以通过将经解密的支付信息发送到商家服务器计算机，发起支付交易，然后商家服务器计算机可以使用经解密的支付信息来生成用于支付交易的授权请求消息。在其他实施例中，商家应用程序可以被配置成生成授权请求消息，并将授权请求消息发送到商家服务器以供处理。

[0066] 另外，在一些实施例中，商家应用程序可以由收单方、支付服务提供商或代表一个或多个商家来操作和/或处理一个或多个商家的远程交易的后端处理器操作或与它们相关联。例如，商家应用程序可包括被配置成代表商家计算机来处理远程交易的支付服务提供商。另外，收单方可以代表商家计算机处理交易，并可以提供收单方应用程序，该收单方应用程序通过允许消费者通过收单方应用程序发起远程支付，执行与商家应用程序类似的功能。

[0067] “公钥/私钥对”可包括由实体生成的一对有联系的加密密钥。公钥可以用于公共功能(诸如加密消息以发送到实体)或用于确认由实体声称的数字签名。另一方面，私钥可以用于私有的功能，诸如解密接收到的消息或应用数字签名。公钥通常将被被称为证书颁

发机构的主体授权，该证书颁发机构将公钥存储在数据库中并将它分发到请求它的任何其他实体。私钥通常将被保留安全存储介质中，并通常将被实体或受信任的各方所知。然而，此处所描述的密码系统可以具有用于恢复丢失的密钥并避免数据丢失的密钥恢复机制。

[0068] “公钥”可包括可以被公开地共享的任何加密密钥。公钥可以被设计用于被共享并可以被配置为使得利用公钥加密的任何信息只能被使用与公钥相关联的私钥(即，公钥/私钥对)来解密。

[0069] “私钥”可包括可以被保护且安全的任何加密密钥。例如，私钥可以安全地存储在生成公钥/私钥对的实体上，并可以被用来解密利用公钥/私钥对的相关联的公钥加密的任何信息。

[0070] “数字签名”可以是指应用允许签名方声明以及确认方确认文档的可靠性和完整性的算法的结果。例如，对于公钥/私钥对，签名方可以通过私钥来操作，而确认方可以通过公钥来操作。由于不允许否认所签名的东西的所谓的不可否认性的原理，此过程可以证明发送方的可靠性和签名的文档的完整性。包括签名方的数字签名的证书或其他数据被称为是被签名方“签名的”。

[0071] “证书”可包括确定实体的身份和/或真实性的电子文档或数据文件。例如，证书可以使用数字签名来将公钥和与身份相关联的数据绑定。证书可包括一个或多个数据字段，诸如身份的合法名称、证书的序列号，证书的有效期的截止日期，证书相关的权限，或标识和/或认证实体或证书本身的任何其他相关信息。例如，证书可以包含“有效起始日”日期表示证书有效的第一日期，而“有效截止日”日期表示证书有效的最后日期。进一步，证书也可以包括包含数据字段的证书中的数据的散列。另外，每一证书都可以由证书颁发机构签名。

[0072] “证书颁发机构”可包括被配置成发行证书的任何实体。证书颁发机构可以使用包括证书颁发机构的公钥的证书颁发机构证书来证明其身份。证书颁发机构证书可以由另一证书颁发机构的私钥签名，或可以由同一证书颁发机构的私钥签名。后者被称为自我签名的证书。证书颁发机构通常还维护由该证书颁发机构颁发的所有证书的数据库。

[0073] 在典型的证书颁发过程中，证书颁发机构从其身份已知的实体接收未签名的证书。未签名的证书包括公钥、一个或多个数据字段，和证书中的数据的散列。证书颁发机构可以利用对应于证书颁发机构证书上包括的公钥的私钥，对证书进行签名。然后，证书颁发机构可以将经签名的证书存储在数据库中，并向实体颁发经签名的证书。此后，实体可以使用证书作为用于呈现实体的真实性和身份的装置。

[0074] 在一些实施例中，证书颁发机构可包括来自交易处理生态系统的实体中的任何一个。例如，支付处理网络、远程密钥管理器、发行方、收单方，或交易系统内的任何其他实体也可以负责颁发和证明证书。例如，商家、商家应用程序、或被配置成处理远程交易的收单方计算机可以向远程密钥管理器、支付处理网络、移动钱包提供商或任何其他第三方注册，以便获取由相应的实体签名的允许该实体验证证书并确保证书对任何给定交易有效的公钥证书。在一些实施例中，远程支付交易处理系统内的实体可以联络证书颁发机构，以判断证书的状态是否被更新，处于存续期，被撤销，等等。相应地，证书颁发机构可以被配置成提供关于颁发的证书的状态信息。

[0075] “服务器计算机”可包括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机，微型计算机集群或充当一个单元的服务器组。在一个示例中，服务器计算机可以是

耦合到web服务器的数据库服务器。服务器计算机可以耦合到数据库，并可以包括任何硬件、软件、其他逻辑，或用于服务于来自一个或多个客户端计算机的请求的前面各项的组合。服务器计算机可以包括一个或多个计算设备，并可以使用用于服务于来自一个或多个客户端计算机的请求的各种计算结构、布局，以及编译中的任何一种。

[0076] 如那些精通本技术的普通人员将认识到的，此处所描述的本发明的各实施例包括可以以任何合适的方式组合的多个不同的各实施例。例如，在下面所描述的各实施例中，描述了各种不同的方、商家应用程序、移动支付应用程序，以及交易处理器，并作为示例，提供了特定流程图。这些示例是为说明本发明的概念而提供的，并是非限制性的。相应地，可以以任何合适的方式组合来自各实施例的特征，包括以与在此处所描述的每一说明性系统中显式地提供的配置不同的配置来使用已注册的公钥和公钥证书。相应地，这只是可以根据下面可以比较详细地描述的本发明的一些实施例提供的各种组合的一个示例。进一步地，关于可能可用的各种配置选项的额外的信息可以在2014年7月15日提交的美国非临时申请案No.14/332,245中发现，在此为各种目的完整地包括了该申请作为参考。

[0077] I.示例性系统

[0078] 图1示出了根据本发明的一些实施例的用于使用远程密钥管理器140和移动设备120的商家应用程序121来执行远程交易的示例性系统100的框图。系统100包括用户(例如，消费者110)、包括商家应用程序121、安全元件122、远程交易应用程序124以及移动支付应用程序123的通信设备(例如，移动设备120)、远程密钥管理器140、证书颁发机构180、商家计算机130、收单方计算机150、支付处理网络160、目录服务器190、认证计算机191以及发行方计算机170。各种实体可以被配置成通过任何合适的无线或有线通信网络并使用任何合适的通信协议(包括开放的或专有的通信协议)彼此进行通信。

[0079] “发行方”通常可以是指维护用户的财务账户并常常向用户颁发诸如信用卡或贷记卡之类的便携式消费者设备的业务实体(例如，银行)。发行方也可以向移动设备120发行或供应账户信息以允许由移动设备发起的移动支付。“商家”通常是参与交易并可以销售货物或服务的实体。“收单方”通常是与特定商家或其他实体具有业务关系的业务实体(例如，商业银行)。某些实体可以执行发行方和收单方两种功能。一些实施例可以涵盖这样的单一实体发行方-收单方。实体中的每一个都可以包括一个或多个计算机设备(例如，商家计算机130、收单方计算机150、支付处理网络160，以及发行方计算机170)，以实现通信或执行本文所描述的功能中的一项或多项。

[0080] 支付处理网络160可以包括用于支持和递送证书颁发机构服务、授权服务、异常文件服务，交易评分服务，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160可以包括VisaNetTM。诸如VisaNetTM之类的支付处理网络能够处理信用卡交易、借记卡交易，及其他类型的商业交易。具体而言，VisaNetTM包括处理授权请求的VIP系统(集成Visa的支付系统)以及执行清算和结算服务的Base II系统。

[0081] 支付处理网络160可包括一个或多个服务器计算机161。服务器计算机通常是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机，微型计算机集群或充当一个单元的服务器组。在一个示例中，服务器计算机可以是耦合到web服务器的数据库服务器。支付处理网络160可以使用任何合适的有线或无线网络，包括因特网。

[0082] 在某些“卡存在”或店内支付交易中，用户使用移动设备120在商家处购买商品或

服务。例如，用户的移动设备120可以在与商家计算机130相关联的商家处与访问设备(未示出)进行交互。例如，用户可以对着访问设备中的近场通信(NFC)读取器敲击移动设备120。可另选地，在远程或“卡不存在”交易中，用户可以以电子方式向商家计算机130指出支付详细信息，诸如在在线交易中。

[0083] 授权请求消息可以由移动设备120或商家计算机130生成，然后被转发到收单方计算机150。在接收到授权请求消息之后，然后将授权请求消息发送到支付处理网络160。然后，支付处理网络160将授权请求消息转发到与与用户相关联的发行方相关联的对应的发行方计算机170。

[0084] “授权请求消息”可以是发送到支付处理网络160和/或支付卡的发行方以请求对于交易的授权的电子消息。根据一些实施例的授权请求消息可以符合ISO 8583，该标准是交换与由用户使用支付设备或支出账户作出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以与支付设备或支付账户相关联的发行方账户标识符。授权请求消息也可以包括对应于“标识信息”的附加数据元素，包括，只作为示例：服务代码、CVV(卡验证值)、dCVV(动态卡验证值)、有效期等等。授权请求消息也可以包括“交易信息”，诸如，与当前的交易相关联的任何信息，诸如，交易量、商家标识符、商家位置，等等，以及可以用于判断是否标识和/或授权交易的任何其他信息。授权请求消息也可以包括其他信息，诸如标识生成了授权请求消息的访问设备的信息，有关访问设备的位置的信息，等等。

[0085] 在发行方计算机170接收授权请求消息之后，发行方计算机170将授权响应消息发回到支付处理网络160以指出当前交易是否被授权(或不被授权)。然后，支付处理网络160将授权响应消息转发回到收单方计算机150。在一些实施例中，例如根据诈骗风险评分值，即使发行方计算机170授权了交易，支付处理网络160也可以拒绝该交易。然后，收单方计算机150将响应消息发送到回到商家计算机130。

[0086] “授权响应消息”可以是对由发行金融机构170或支付处理网络160所生成的授权请求消息的电子消息回复。仅作为示例，授权响应消息可以包括下列状态指示符中的一个或多个：“批准”--交易得到批准；“拒绝”--交易未被批准；或“呼叫中心”--响应因需更多信息而待决，商户必须呼叫免付费的授权电话号码。授权响应消息也可以包括授权代码，该授权代码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(直接或者通过支付处理网络160)返回到商家计算机130的指出交易的批准的代码。该代码可以充当授权的证明。如上文所指出，在一些实施例中，支付处理网络160可以生成授权响应消息或将其转发给商家。

[0087] 在商家计算机130接收到授权响应消息之后，商家计算机130可以向用户提供授权响应消息。响应消息可以由移动设备120显示，或可以打印在物理收据上。可另选地，如果交易是在线交易，则商家可以提供网页或授权响应消息的其他指示作为虚拟收据。收据可包括针对交易的交易数据。

[0088] 在一天结束时，可以由支付处理网络160进行正常的清算和结算过程。清算过程是在收单方和发行方之间交换财务细节的过程以促进向消费者的支付账户的过帐和用户的结算位置的核对。

[0089] 在图1的远程交易处理系统中，移动设备120被配置成使用远程密钥管理器140，发起并处理与商家计算机130的远程交易，以提供安全的远程支付交易环境，甚至在使用安装

在通信设备(例如,移动设备120)的未知商家应用程序121或其他移动应用程序的情况下。

[0090] 用户(例如,消费者110)可以操作通信设备(例如,移动设备120)以执行移动设备120被配置成执行的任意数量的功能。例如,消费者110可以使用移动设备120,通过与远程密钥管理器140和商家计算机130进行通信,来执行远程支付交易。商家计算机130可以将可用的产品和服务提供到消费者110可以用来发起远程交易的商家应用程序121,无论位于商家位置处或远离商家。

[0091] 通信设备(例如,移动设备120)可以被配置成与被配置成促进和/或处理远程交易的远程密钥管理器140进行通信。远程密钥管理器140被配置成执行与远程交易相关的许多功能,包括接收经加密的支付信息,验证与远程交易相关联的公钥证书,使用远程密钥管理器密钥来解密经加密的支付信息,通过任意数量的认证过程来验证安全信息,以及使用与用于交易的交易处理器(例如,商家、商家处理器、收单方等)相关联的公钥来重新加密支付信息。在图3中更详细地描述了远程密钥管理器140的各种模块。

[0092] “通信设备”可包括任何电子计算设备。例如,“通信设备”可包括移动设备120,移动设备120可包括移动电话、平板、上网本、膝上型计算机,或任何其他合适的移动计算设备。移动设备120可以包括商家应用程序121、远程交易应用程序124,以及移动支付应用程序123。移动支付应用程序123和远程交易应用程序124可以存储在安全存储器(例如,安全元件122)中。

[0093] 商家应用程序121可包括任何移动程序、软件,或适合于执行支付交易的其他合适的可执行代码。在一些实施例中,商家应用程序121可以是商家特定的应用程序。在其他实施例中,商家应用程序121可以是通用应用程序,诸如web浏览器。进一步,商家应用程序121可以与不是商家而是代表商家或其他服务提供商(例如,支付服务提供商、收单方,等等)处理支付的各方相关联。

[0094] 安全元件122可以是可操作以安全地存储任何信息和/或安全应用程序的任何硬件或软件部件。例如,安全元件122可以是可操作以存储支付信息。安全元件122是受信任的执行环境(TEE)的示例。受信任的执行环境可以通过使用软件或硬件元件来实现,并可以存在于通信设备或远程服务器计算机(例如,基于云的TEE)上。进一步,可以提供移动支付应用程序123并将其存储在安全元件122上,以安全地访问与消费者的财务账户相关联的个性化敏感信息(例如,支付凭证、令牌、账户标识符,等等)。例如,在一些实施例中,安全元件122可包括安全的加密处理器或免接触集成电路以保护存储在安全元件122上的信息。安全元件122可以具有单独的处理器,存储在其上的信息可以利用只有受信任的服务管理器或其他指定的实体持有的秘密密钥来加密,而安全元件122可以包含任何其他硬件,以便安全元件122可以是可以存储重要信息(例如,支付凭证、加密密钥,以及任何其他敏感信息)的安全区域。进一步,可以使用某些受信任的服务管理器可以管理的特殊秘密密钥,来访问安全元件122的安全数据元素。

[0095] 另外,在一些实施例中,可以由远程服务器计算机提供受信任的执行环境,该受信任的执行环境允许通过与此处所描述的过程类似的过程,向移动支付应用程序传送敏感信息,而不使用安全元件或通信设备上的其他受信任的执行环境。例如,可以在交易之前向通信设备传送在有限的时间段内有效的敏感信息允许如此处所描述的类似的过程被执行,而不要求安全元件或其他硬件实现的受信任的执行环境在通信设备上存在。

[0096] 商家应用程序121可包括远程交易SDK(未示出)或第三方服务层,该第三方服务层可包括适合于与远程交易应用程序124和/或第三方服务器系统接口应用程序(例如,移动钱包提供商、移动网关、远程密钥管理器140,等等)连接的任何API、应用程序、小程序,或其他可执行代码。例如,远程交易SDK可以被嵌入在商家应用程序121中,并可以被商家应用程序121用来从安全元件122上的远程交易应用程序124中检索支付信息,以便与在安全元件122上提供的移动支付应用程序123连接。另外,虽然远程交易SDK被描述为是商家应用程序121的一部分,但是,远程交易SDK也可以是独立应用程序或可以被嵌入到移动设备120的操作系统中。

[0097] 远程交易应用程序124包括被供应到移动设备120的安全元件122中的安全应用程序。远程交易应用程序124提供安全区域,用于存储公钥证书和/或第三方计算机系统(例如,远程密钥管理器140、移动钱包提供商、移动网关,等等)的其他加密密钥。远程交易应用程序124(也被称为远程交易小程序)可以被配置成与移动支付应用程序123(例如,VisaTMPaywaveTM应用程序)或存储在通信设备(例如,移动设备120)的安全元件122上的其他支付应用程序进行通信。另外,远程交易应用程序124还可以被配置成与远程密钥管理器140或被配置成安全地促进远程支付交易的发起和认证的其他第三方系统进行通信。

[0098] 因此,当消费者110提供了安全凭证或以别的方式被认证时,远程交易应用程序124可以通过允许对移动支付应用程序123的访问,提供移动支付应用程序123的访问控制确认(例如,提供移动支付应用程序123的安全功能)。例如,如果与商家证书相关联的签名不能被验证或如果证书不与证书颁发机构180匹配,则远程交易应用程序124可以拒绝来自商家应用程序121的对远程交易的请求,交易处理可以结束(并可以提示消费者110尝试不同的支付方式或再次尝试)。可另选地,如果证书有效,则远程交易应用程序124可以将对支付信息的请求传递到移动支付应用程序123。

[0099] 移动支付应用程序123可包括任何应用程序编程接口(API)、服务、应用程序、小程序,或适合于从安全存储模块或安全元件122检索支付信息并与商家应用程序121进行通信的其他可执行代码。在一些实施例中,移动支付应用程序123可以被安全保护。例如,移动支付应用程序123可以在安全元件122(如图2所示)或其他受信任的环境中作为内核服务运行,或在比商家应用程序121更高权限级别运行。

[0100] 移动支付应用程序123可包括与远程密钥管理器140相关联的证书,该证书可以被用来使用与远程密钥管理器140相关联的公钥(或其他加密密钥)加密支付信息及其他通信。在一些实施例中,移动支付应用程序123可以可操作以生成与支付信息相关联的安全值(例如,密码)。例如,移动支付应用程序123可以可操作以生成包括与支付账户相关联的动态卡确认值(dCVV2)的安全值。在其他实施例中,移动支付应用程序123可以能够生成特定的动态认证请求或可以被与个性化移动支付应用程序123共享秘密的支付处理网络160验证的其他动态值。

[0101] 图2示出了根据本发明的一些实施例的示例性通信设备(例如,移动设备120)的框图。移动设备120可包括用于实现某些设备功能(诸如电话)的电路。负责实现这些功能的功能元件可包括被编程为执行实现设备的功能和操作的指令的处理器120(A)。处理器120(A)可以访问数据存储120(E)(或另一合适的存储器区域或元件)以检索指令或用于执行指令的数据,诸如商家应用程序、远程交易应用程序124,或其他移动应用程序。诸如键盘或触摸

屏之类的数据输入/输出元件120(C)可以被用来使用户能操作移动设备120并输入数据(例如,用户认证数据)。数据输入/输出元件也可以被配置成输出数据(例如,通过扬声器)。显示器120(B)也可以被用来向用户输出数据。通信元件120(D)可以被用来在移动设备120和有线或无线网络之间实现数据传输(例如,通过天线120(H))以帮助连接到因特网或其他通信网络,并实现数据传输功能。

[0102] 移动设备120还可以包括免接触元件接口或安全存储器接口120(F)以在免接触元件120(G)及设备的其他元件之间实现数据传输,其中,免接触元件120(G)可包括安全存储器(例如,安全元件122)和近场通信数据传输元件(或另一形式的短距离或免接触通信技术)。如所指出的,蜂窝电话或类似的设备是根据本发明的各实施例可以使用的通信设备(例如,移动设备120)的示例。然而,其他形式或类型的设备可被使用而不脱离本发明的底层概念。进一步,设备为了适合与本发明的实施例一起使用而可不需要使用蜂窝网络来通信的能力。

[0103] 图3示出了根据本发明的一些实施例的示例性远程密钥管理器140的框图。远程密钥管理器140可以包括服务器计算机141、私钥数据库141(G),以及证书颁发机构根公钥数据库141(H)。服务器计算机141可以包括证书确认模块141(A)、公钥提取模块141(B)、交易处理模块141(C)、安全信息验证模块141(D)、通信设备接口141(E),以及支付处理网络接口141(F)。服务器计算机141还可以进一步包括处理器(未示出)以及耦合到处理器的计算机可读取的介质(未示出),计算机可读介质包括可由处理器执行的用于执行如此处的各实施例所描述的方法的代码。

[0104] 证书确认模块141(A)可包括可以被配置成将商家证书(或其他交易处理器证书)确认为与特定商家相关联,是真实的,和/或有效的任何软件模块。证书确认模块141(A)可以执行任意数量的步骤,以便实现此功能。例如,证书确认模块141(A)可以与证书颁发机构180进行通信,以确保公共证书当前有效并在存续期内(例如,未被通过证书吊销列表(CRL)或在线证书状态协议响应器(CSPR)等等报告为被损坏或撤销)。另外,证书确认模块141(A)可以使用存储在证书颁发机构公共根密钥数据库141(H)中的证书颁发机构根公钥来验证公钥证书是合法的,并由合适的证书颁发机构180签名。

[0105] 返回到图1,证书颁发机构180可以与远程密钥管理器140相关联,以允许对证书的状态的验证。另外,证书颁发机构还可以与商家计算机130相关联并可以向商家计算机130发行公钥证书,可以在远程支付交易处理过程中使用该公钥证书以在第三方服务器计算机(例如,远程密钥管理器140)和商家计算机130之间建立信任,该信任为商家计算机130是可靠的并且被授权获取经加密的支付信息中的敏感的支付凭证。在下面的图5中比较详细地描述了证书颁发机构180可以发行商家证书的过程。可在ANSI X9.24部分2零售金融服务对称密钥管理部分2:使用对称密钥的分配的非对称技术(ANSI X9.24 Part2Retail Financial Services Symmetric Key Management Part 2:Using Asymmetric Techniques for the Distribution of Symmetric Keys)以及ISO 11568部分4银行业—密钥管理(零售)—部分4:非对称密码系统—密钥管理和生命周期(ISO 11568Part 4Banking—Key management(retail)—Part 4:Asymmetric cryptosystems—Key management and life cycle)中找到证书发行方法的一些非限制性示例。

[0106] 公钥提取模块141(B)可以被配置成从接收到的或存储的公钥证书中提取用于处

理远程交易的公钥。可以使用任何合适的过程来提取公钥。在一些实施例中，可以在对公钥证书的验证和/或确认之前或之后提取公钥。

[0107] 交易处理模块141(C)可以被配置成处理支付请求并且作为对支付请求的回复而提供支付响应，假设接收的或储存公共密钥证书对于交易是有效的且积极的。例如，交易处理模块141(C)可以使用存储在私钥数据库141(G)中的远程密钥管理器私钥来解密接收到的经加密的消息，并使用从交易处理器证书(例如，商家证书)提取的交易处理器公钥来重新加密经解密的消息或来自消息的信息，以便安全传送到交易处理器(例如，商家计算机130)。交易处理模块141(C)还可以进一步将经重新加密的消息(例如，支付响应)传递到通信设备(例如，移动设备120)，以便传递到合适的交易处理器(例如，商家计算机130)。

[0108] 安全信息验证模块141(D)可包括被配置成发起与支付处理网络160的认证通信以便发起认证过程的任何软件模块。例如，安全信息验证模块141(D)可以被配置成使用支付处理网络接口141(F)，将包括安全信息的认证请求发送到与经解密的支付信息相关联的支付处理网络服务器计算机161。支付处理网络服务器计算机161可以确定与经解密的支付信息相关联的认证计算机191，并将认证请求转发到认证计算机191。然后，认证计算机191可以验证安全信息，并生成包括认证响应值的认证响应。然后，安全信息验证模块141(D)可以通过支付处理网络接口141(F)，从支付处理网络计算机161接收包括认证响应值的认证响应。

[0109] 在一些实施例中，其中远程密钥管理器计算机141可以与支付处理网络160相关联，远程密钥管理器140可以被配置成通过将目录服务器功能并入远程密钥管理器140来确定与远程支付交易相关联的认证计算机191。相应地，远程密钥管理器计算机的安全信息验证模块141(D)可以确定与经解密的支付信息相关联的认证计算机191，并可以将包括安全信息的认证请求发送到认证计算机191。认证计算机191可以验证安全信息，并返回指出对安全信息的验证的包括认证响应值的认证响应。

[0110] 通信设备接口141(E)可以被配置成与通信设备(例如，移动设备120)进行通信。例如，通信设备接口141(E)可以包括任何合适的通信协议或网络接口，以便与移动设备120进行通信。移动设备接口141(D)可以从移动设备120接收消息(例如，支付请求)，可以被配置成解析该消息以确定消息中所包括的相关信息。

[0111] 支付处理网络接口141(F)可包括被配置成将请求传递到支付处理网络160的硬件和/或软件接口。支付处理网络接口141(F)可包括允许信息与支付处理网络160的安全交换的安全信道。例如，可以交换硬件安全接口或基于会话的密钥以确保与支付处理网络服务器计算机161的高度安全的连接。

[0112] 私钥数据库141(G)可以包括远程密钥管理器140的私钥(也被称为远程密钥管理器私钥)。可以通过任何合适的方式生成私钥，并可以安全地存储它，以便不给未经授权的实体提供对私钥的访问。在一些实施例中，私钥可以存储在本地存储器或存储在远程安全数据库中。在一些实施例中，私钥可以是与远程密钥管理器140相关联的私钥/公钥对中的一个，公钥可以被提供给商家应用程序121、移动支付应用程序123、移动设备120、远程交易应用程序(未示出)，以及被配置成加密支付信息供远程密钥管理器140进行处理的任何其他交易实体。另外，在一些实施例中，私钥数据库141(G)可包括对称的加密密钥，在数据是使用对称的加密密钥而不是公共/私有的加密密钥对加密的情况下，可以使用对称的加密

密钥。

[0113] 根公钥数据库141(H)可以包括与公钥证书相关联的证书颁发机构180的根公钥。在一些实施例中，单一证书颁发机构根公钥可以存储在与单一证书颁发机构180相关联的远程密钥管理器140中(并可以本地地存储在远程密钥管理器计算机中)，而在其他实施例中，多个证书颁发机构根密钥可以存储在数据库中，或本地地存储在远程密钥管理器计算机中。证书颁发机构根公钥可以用于签名验证过程中，以确保公钥证书与发行证书机构是有效的且积极的。

[0114] 图4示出了根据本发明的一些实施例的示例性支付处理网络160的一些部件的框图。支付处理网络160可以包括服务器计算机161、发行方认证配置数据库161(E)、以及发行方共享的秘密数据库161(F)。服务器计算机161可以包括安全信息验证模块161(A)、交易处理模块161(B)、目录服务器接口模块161(C)，以及远程密钥管理器接口模块161(D)。服务器计算机161还可以进一步包括处理器(未示出)以及耦合到处理器的计算机可读取的介质(未示出)，计算机可读介质包括可由处理器执行的用于执行如此处的各实施例所描述的方法的代码。

[0115] 安全信息验证模块161(A)可包括配置成验证与支付请求相关联的安全信息(例如，用户认证数据、安全值，或任何其他认证信息)的任何软件模块。例如，安全信息验证模块161(A)可以被配置成确定与认证请求相关联的认证计算机191，并将认证请求转发到相关认证计算机191。安全信息验证模块161(A)可以使用可以通过目录服务器接口模块161(C)访问的目录服务器，确定认证计算机191。

[0116] 返回到图1，在一些实施例中，目录服务器计算机190可以被用来确定被配置成验证给定远程交易的安全信息的认证计算机191。目录服务器190可包括配置成接收认证请求、确定与认证请求相关联的认证计算机191、并将认证请求转发到认证计算机191的任何计算机、设备，和/或系统。例如，目录服务器可包括其中包括与支付账户相关联的发行方标识符以及为每一个发行方标识符指定的对应的认证计算机的发行方认证配置数据库161(E)。例如，目录服务器可以包括与支付处理网络160相关联的银行标识号码(BIN)(例如，VisaNet™)的列表以及与每一BIN相关联的对应的认证计算机地址。例如，认证计算机地址可包括IP地址、HTTP地址、内部目录地址，或允许目录服务器确定并提供认证请求要被转发到的合适的位置以确保正确的认证计算机191接收并验证安全信息的任何其他信息。

[0117] 认证计算机191可包括被配置成接收包括与远程支付交易相关联的安全信息的认证请求、验证安全信息，并提供指出安全信息被验证和/或认证的认证响应值的任何计算机、系统、设备，或设备的组合。认证计算机可包括认证数据库，其中包括个人信息、用户名、密码、PIN、口令、共享的机密，以及允许系统认证用户具有执行交易的授权或权限的任何其他相关信息。

[0118] 认证计算机191可以由支付处理网络160、发行方，或由第三方相关联和/或操作。例如，账户发行方可以向支付处理网络160或其他第三方计算机系统提供发行方简档信息(例如，认证规则、风险规则，等等)以及与账户持有人、设备相关联的共享的机密，以及任何其他相关信息，以允许支付处理网络或其他实体执行对安全信息的认证。这样的系统可以被视为“代表”认证系统，其中，发行方提供向第三方认证信息以允许认证功能由代表发行方的第三方执行。与账户发行方相关联或由其管理的认证计算机191可以被视为访问控制

服务器(ACS)。

[0119] 在一些实施例中,认证计算机191也可以包括与授权决定过程相关联的发行方计算机170。因此,在一些实施例中,支付处理网络161可以按与支付交易处理类似的方式将认证请求发送到发行方计算机170(例如,通过使用ISO消息或其他预先配置的与发行方计算机的接口)。

[0120] 进一步,在一些实施例中,在远程交易认证过程中可以使用一个以上的认证计算机191。例如,支付处理网络160可以通过账户发行方与由支付处理网络160操作的"代表"认证计算机共享与账户相关联的共享的秘密,代表账户发行方执行设备认证。然而,账户发行方可以不利用支付处理网络160提供消费者简档信息以及对应的用户认证数据,而是,用户认证数据可以被传递到发行方认证计算机191、访问控制服务器(ACS),或被配置成认证消费者信息的其他计算机。因此,支付处理网络160可以与验证用户认证数据的发行方的访问控制服务器(ACS)并行地或结合地验证设备认证信息。

[0121] 另外,在一些实施例中,支付处理网络认证计算机可以将认证结果传递到账户发行方访问控制服务器计算机(即,与发行方相关联的认证计算机)。例如,传递到认证计算机191的安全信息可包括安全值(例如,密码)和/或用户认证数据(例如,口令)预先由代表账户发行方170的支付处理网络160认证的指示。相应地,在一些实施例中,与账户发行方170相关联的认证计算机191可以参与认证响应值或对消费者和/或设备的认证的其他指示的生成,而不执行对安全信息的直接验证。进一步,在一些实施例中,基于由与账户发行方170相关联的认证计算机191对安全信息的验证,与支付处理网络160相关联的认证计算机生成认证响应值的角色可以颠倒。

[0122] 认证计算机191可以使用共享的机密或共享的算法来验证使用可重复的输入数据来重复计算的安全值,并比较交易的动态安全值(例如,密码)。例如,安全值(例如,密码)可以由移动支付应用程序123使用账户标识符、到期日期、交易时间、交易金额,或可以对移动支付应用程序123和与账户发行方计算机170和/或支付处理网络160(或任何其他处理实体)相关联的认证计算机191两者可用的任何其他合适的交易信息来生成。例如,可以在移动支付应用程序123和与支付处理网络160相关联的认证计算机191或账户发行方计算机170或其他处理实体之间共享算法,以便允许对安全信息的验证。

[0123] 相应地,返回到图4,在一些实施例中,安全信息验证模块161(A)可以使用目录服务器接口模块161(C),将通过远程密钥管理器接口模块161(D)从远程密钥管理器140接收到的认证请求转发到与支付请求相关联的目录服务器计算机190。

[0124] 目录服务器接口模块161(C)可包括被配置成将认证请求和响应传递到目录服务器计算机190或系统的硬件和/或软件接口。目录服务器接口模块161(C)可包括允许信息与目录服务器计算机190的安全交换的安全信道。例如,可以交换硬件安全接口或基于会话的密钥以确保与目录服务器计算机190的高度安全的连接。

[0125] 然而,在其他实施例中,目录服务器的功能可以被包括到支付处理网络160(和/或远程密钥管理器140)中,以便支付处理网络160(或远程密钥管理器计算机)可以基于认证请求中所包括的信息来确定合适的认证计算机191。例如,支付处理网络计算机可以通过从认证请求解析账户凭证(例如,主账户号码、令牌或账户代用品,等等)并确定与账户凭证相关联的发行方,确定与认证请求相关联的认证计算机191。例如,在一些实施例中,认证请求

可包括与远程支付交易相关联的主要账户号码(PAN),PAN可包括与账户的发行方相关联的银行标识符(例如,BIN)。相应地,安全信息验证模块161(A)可以将BIN与发行方认证配置数据库161(E)进行比较,以确定与发行方的账户相关联的认证计算机191。进一步地,发行方可以具有被不同的认证计算机认证的某些账户,如此,在一些实施例中,目录服务器可以确定与账户范围相关联的认证计算机191或与发行方相关联的帐号。

[0126] 发行方认证配置数据库161(E)可包括与确定与账户和/或账户发行方相关联的认证计算机191相关的任何信息。发行方认证配置数据库161(E)也可以包括与发行方相关联的认证偏好,以及与账户发行方相关联的用于风险确定、交易处理,授权决策,等等的简档信息。进一步地,取决于系统的配置选项,可以在支付处理网络160或在目录服务器上发现发行方认证配置数据库161(E)。

[0127] 发行方共享的秘密数据库161(F)可包括允许实体验证安全信息和/或与发行方账户相关联的其他认证信息的任何信息。例如,在一些实施例中,共享的秘密数据库可包括用于重复生成与账户相关联的安全值的共享的秘密算法,或可包括相关消费者认证和设备认证信息的可搜索的数据库。

[0128] 进一步,安全信息验证模块161(A)可以被配置成使用安全地存储在支付处理网络160中的秘密算法,生成认证响应值,秘密算法可以不被与远程交易处理系统中的任何其他实体共享。相应地,安全信息验证模块161(A)可以验证由移动支付应用程序123生成的动态密码(例如,安全值),并可以返回可以被返回到移动设备120并与为交易生成的任何授权请求消息一起提交的另一动态密码(例如,认证响应值)。相应地,支付处理网络160可以在对授权请求消息的交易处理过程中获取认证响应值,并可以验证认证响应值匹配在对远程支付交易的初始处理过程中由支付处理网络160最初生成的认证响应消息。相应地,可以向支付处理网络160确保交易未被改变并且交易数据与最初被支付处理网络计算机161认证的交易相同。

[0129] 交易处理模块161(B)可包括被配置成接收授权请求消息并为交易处理授权请求消息的任何软件模块。上文说明了关于授权请求消息的处理的更多细节。

[0130] 远程密钥管理器接口模块161(D)可包括被配置成允许支付处理网络160与远程密钥管理器140连接的软件和/或硬件接口。远程密钥管理器接口模块161(D)可包括允许信息与远程密钥管理器计算机的安全交换的安全信道。例如,可以交换硬件安全接口或基于会话的密钥以确保与远程密钥管理器服务器计算机141的高度安全的连接。支付处理网络160可以通过远程密钥管理器接口模块161(D)从远程密钥管理器140接收认证请求,并通过远程密钥管理器接口模块161(D),将认证响应发送到远程密钥管理器190(或取决于配置,其他实体,例如,移动网关)。

[0131] A.商家证书发行/供应方法

[0132] 图5示出了根据本发明的某些实施例的用于使用证书颁发机构180来给商家供应公钥/私钥对和商家应用程序证书的示例性方法500的流程图。在一些实施例中,方法500可以被执行以便给商家计算机130提供指出商家的可信赖性或可靠性的证书。随后,接收到的商家证书可以被包括在安装在移动设备上或提供给移动设备的商家应用程序中。

[0133] 在步骤501中,商家计算机130生成商家公钥私钥对。可以以任何合适的格式(诸如RSA或椭圆曲线加密(ECC))来生成商家公钥私钥对。在一些实施例中,商家私钥可以安全地

存储在商家计算机130上。

[0134] 在步骤502中，商家计算机130将公钥私钥对的商家公钥发送到证书颁发机构180。证书颁发机构180可包括配置成发行并验证证书的任何合适的实体。例如，在一些实施例中，证书颁发机构180可包括支付处理网络160、远程密钥管理器140、移动钱包提供商、未包括在典型的支付交易处理系统内的实体，或任何其他实体。

[0135] 在步骤503中，证书颁发机构180使用任何合适的手段来确认商家的真实性。例如，商家计算机130可以给证书颁发机构180提供信息，该信息提供正在由商家操作的商家计算机130的身份。在一个示例中，商家计算机130可以提供由商家的经授权的签署人(例如，商家组织的总裁)签名的文档。

[0136] 在步骤504中，证书颁发机构180使用包括商家公钥的接收到的商家证书签名请求来生成经签名的商家证书。通常，商家证书可以由证书颁发机构根私钥签名。证书颁发机构签名允许实体使用证书颁发机构根公钥来验证商家证书的可靠性。

[0137] 在步骤505中，证书颁发机构180将经签名的商家证书发送到商家计算机130。

[0138] 在步骤506中，商家计算机130使用商家私钥来生成经签名的商家应用程序证书。如此，可以建立从商家应用程序证书，到商家证书，到证书颁发机构根证书的信任的链。在一些实施例中，经签名的商家应用程序证书可以与商家应用程序121的实例或版本相关联。例如，商家应用程序证书可以被用来确认商家应用程序121来自于该商家。

[0139] 在步骤507中，商家计算机130将商家应用程序证书存储在商家应用程序121中。如此，当商家应用程序121被加载到移动设备120中时，可以确认商家应用程序121的可靠性。另外，商家计算机130可以本地地存储与商家应用程序证书相关联的商家应用程序私钥，以允许对使用商家应用程序公钥加密的信息的解密。

[0140] 应该理解，图5只是描述性的而非限制性的。例如，在本发明的一些实施例中，商家公钥-私钥对可以由证书颁发机构180生成，例如，可以使用公钥加密标准(PKCS)#12消息将商家私钥安全地提供到商家计算机130。进一步地，在一些实施例中，可以使用类似的技术来生成与商家服务器计算机或安全交易处理系统内的其他实体相关联的商家证书。

[0141] B.示例性方法

[0142] 图6示出了根据本发明的一些实施例的用于使用远程密钥管理器140和移动设备120的商家应用程序121来处理远程交易的示例性方法600的流程图。在一些实施例中，可以在提供商家应用程序证书(例如，根据方法500)并与商家应用程序私钥一起或没有商家应用程序私钥地存储在商家应用程序121中之后执行图6的方法。随后，可以执行图6的方法，以便执行对于商品或服务的远程支付交易。

[0143] 如上所述，各实施例允许与支付处理网络160连接，这会提供多个优点，包括附加的认证能力，包括在使用授权请求消息通过支付网络向支付处理网络160提交交易之前，对认证值的验证。相应地，支付处理网络160可以在发起支付之前，对支付请求(以及相关联的消费者账户)执行附加认证过程(例如，风险管理、速度检查等等)，这可以允许支付处理网络160在通过授权请求消息发起支付交易之前，通知商家系统交易是否是可靠的。随后，商家可以基于由支付处理网络160所提供的认证结果，改变风险确定、认证过程，以及任何其他交易过程。

[0144] 另外，通过与支付处理网络160连接，支付处理网络160可以通过生成授权响应值

允许附加一层的交易认证，在交易被授权之前，可以由支付处理网络160验证该授权响应值。进一步地，通过与支付处理网络160连接，远程密钥管理器140可以充当认证系统的单一接口点，允许对与远程交易相关联的用户以及设备的有效率的认证。由于远程本质以及商家或其他亲自的服务提供商缺乏能力认证消费者110，双认证对于远程支付交易特别重要。

[0145] 在步骤601中，消费者110通过与商家计算机130或主控在线或电子商务商店的其他计算机进行通信的通信设备的商家应用程序121来结束他们的购物体验。消费者110可以通过通信设备(例如，移动设备120)的商家应用程序121，发起付款过程。商家应用程序121可以使用远程交易应用程序124，提供远程支付交易的选项，消费者110可以选择远程交易应用程序124作为付款选项。相应地，消费者110使用商家应用程序121，发起远程支付交易，商家应用程序121将指出消费者110愿意发起远程交易的消息发送到商家计算机130。

[0146] 在一些实施例中，商家应用程序121可以提供选择通过远程交易应用程序124进行支付的支付卡或账户的选项。因此，在一些实施例中，远程交易应用程序124可能已经预先确定可用于远程支付交易的可用的卡或账户，并可以将可用的账户信息传递到商家应用程序121。另选地或另外地，当准备付款时或在任何其他合适的时间，商家应用程序121可以请求可用的账户。相应地，在一些实施例中，当通过商家应用程序121发起远程支付时，消费者110可以选择账户。在其他实施例中，可以使用默认账户，或远程交易应用程序124可以提示消费者110在稍后的时间选择一个账户。

[0147] 在步骤602中，商家计算机130接收远程交易发起的指示，并通过生成远程支付交易的交易信息并将其发送到移动设备120的商家应用程序121来作出响应。交易信息可包括，例如，商家标识符、交易金额、交易的认证类型、交易标识符、商家证书，以及用于处理远程交易的任何其他相关信息。

[0148] 另外，在一些实施例中，当付款选项被提供到用户时，交易信息可能已经预先被提供到商家应用程序121。不管怎样，商家应用程序121都可以访问与远程交易相关联的交易信息。

[0149] 在步骤603中，商家应用程序121使用远程交易软件开发工具包(SDK)、远程交易服务层、远程交易应用程序124应用程序编程接口(API)，或位于移动设备120上的任何其他应用程序，将收款人信息发送到远程交易应用程序124。收款人信息可包括适合于标识与远程支付交易相关联的商家的信息(例如，商家证书、与移动支付应用程序123相关联的商家标识符，等等)，用户支付方式(例如，与移动支付应用程序123相关联的支付凭证)，交易类型(例如，远程交易)，以及可以与移动支付应用程序123相关的用于处理远程支付交易的任何其他信息。

[0150] 例如，收款人信息可包括与商家应用程序121或商家计算机130相关联的商家证书。另选地或另外地，收款人信息可包括可以被用来确定存储在移动支付应用程序123中的与商家应用程序121或商家计算机130相关联的商家证书的商家标识符。

[0151] 进一步，收款人信息可包括在注册阶段提供给商家应用程序121(或与商家应用程序121相关联的商家服务器)的用于远程交易处理服务或远程密钥管理器140的商家标识符。在一些实施例中，收款人信息可以被用来标识在其中提供给远程密钥管理器140的商家证书(例如，对于移动支付应用程序123将商家证书传递到远程密钥管理器140的各实施例)。

[0152] 另外，收款人信息可包括交易标识符的类型，通知移动支付应用程序123，请求与远程支付交易相关联。相应地，移动支付应用程序123可以选择用来加密支付信息的合适的加密密钥(例如，远程密钥管理器密钥)，远程密钥管理器140的合适的目的地或路由地址，以及用于与远程密钥管理器140进行通信的正确的通信协议或消息格式。

[0153] 最后，收款人信息还可包括用户的名称、与支付方式(例如，Visa™、MasterCard™等等)相关联的支付处理网络标识符，以及帐号的最后四位，以便移动支付应用程序123标识用于远程支付交易的支付凭证或账户信息。

[0154] 在一些实施例中，此信息中的一些或全部可以由商家应用程序121而不是远程交易应用程序124确定和提供。例如，在商家应用程序121嵌入了API或用于与移动支付应用程序123进行交互的其他软件或可能以别的方式被配置成直接与移动支付应用程序123进行交互的情况下，商家应用程序121可以将远程交易信息(例如，收款人信息、商家证书、交易信息，等等)传递到移动支付应用程序123。不管怎样，远程交易应用程序124都可以接收交易信息、收款人信息，和/或对远程交易中使用的账户的选择。

[0155] 在步骤604中，远程交易应用程序124执行验证控制以及以别的方式确保接收到的交易信息有资格用于远程交易处理。例如，远程交易应用程序124可以确定选定的账户是否被配置成允许远程交易或对应的支付处理网络160是否被配置成允许远程交易。另外，远程交易应用程序124可以验证从商家应用程序121接收到的商家证书，并可以确定是否可以使用证书颁发机构根公钥，来验证商家证书。进一步，远程交易应用程序124可以确保交易信息匹配交易约束(例如，最大交易金额、指定的时段内的交易的最大速度或频率，等等)。

[0156] 进一步地，远程交易应用程序124可以在允许对移动支付应用程序123进行访问之前，要求用户向远程交易应用程序124认证并验证他们的身份。例如，远程交易应用程序124可以请求用户提供与远程交易应用程序124和/或账户的发行方相关联的用户认证数据(例如，共享的秘密、口令，等等)。如果用户不提供用户认证数据或如果用户认证数据不匹配远程交易应用程序124希望的特定格式或类型的信息(例如，使用不被允许或位数太多的符号，等等)，则远程交易应用程序124可以不允许交易进行。可以实现任何附加的确认控制，以便限制对移动支付应用程序123的访问。

[0157] 在步骤605中，如果交易有资格进一步的远程交易处理，则远程交易应用程序124可以将收款人信息传递到安全元件122的移动支付应用程序123。远程交易应用程序124可以使用API或被配置成用于与移动支付应用程序123进行通信的其他命令，以便请求移动支付应用程序123(例如，Visa™ Paywave™应用程序)提供以安全方式存储在安全元件122上的供应的支付凭证(例如，主要账户号码(PAN)、支付令牌、伪PAN、扰乱的PAN、幽灵PAN、到期日期，等等)。

[0158] 在一些实施例中，远程交易应用程序124可以将交易信息转发到移动支付应用程序123。然而，在其他实施例中，交易信息可以存储或保留在远程交易应用程序124中，而从移动支付应用程序123中检索支付凭证。进一步，在一些实施例中，可以由商家计算机130，利用支付处理网络特定的密钥，预先加密交易信息。在这样的实施例中，商家应用程序121、远程交易应用程序124，以及移动支付应用程序123可以不改变交易信息，并可以将预先加密的交易信息与从移动支付应用程序123接收到的经加密的支付信息一起传递到远程密钥管理器140。

[0159] 在其他实施例中，交易信息可以不被预先加密，并可以传递到移动支付应用程序123，以在从移动支付应用程序123返回的经加密的支付信息中加密并包括在其中。进一步，在一些实施例中，交易信息可以不被加密，并可以以未加密的形式与经加密的支付信息包括在一起。

[0160] 在步骤606中，移动支付应用程序123使用接收到的收款人信息来从移动设备120的安全元件122检索和/或生成支付信息。“支付信息”可包括支付凭证(例如，支付帐号(PAN)或令牌)、到期日期、唯一交易标识符(例如，现时值)、安全值(诸如静态或动态卡确认值(dCVV或dCVV2)、密码(例如，ARQC)，或与移动支付应用程序123和支付处理网络160和/或账户发行方之间的共享的秘密相关联的其他安全数据)、安全级别指示符(例如，ECI5值)，或适合于执行远程支付交易的任何其他信息。相应地，移动支付应用程序123可以生成安全信息，包括使用与账户发行方相关联的共享的算法生成的安全值。支付信息还可以包括可以对处理交易有用的任何交易信息(例如，金额、商家标识符，等等)。

[0161] 在生成与支付信息相关联的支付信息之后，移动支付应用程序123使用与远程密钥管理器140相关联的密钥来加密支付信息。例如，移动支付应用程序123可以使用远程密钥管理器密钥或存储在移动支付应用程序123上的其他加密密钥来加密支付信息。远程密钥管理器密钥可以是对称的或者与远程密钥管理器公钥/私钥对相关联的公钥。在一些实施例中，移动支付应用程序123可以使用存储在移动设备120上的远程密钥管理器证书来确定远程密钥管理器公钥，可以从远程密钥管理器140请求证书，或可以获取安全元件122或移动设备120的一般存储器上的远程密钥管理器公钥。在远程密钥管理器密钥是对称密钥的情况下，对称密钥可以与移动支付应用程序123安全地存储在一起。相应地，经加密的支付信息由通信设备的支付应用程序通过访问存储在通信设备的安全存储器中的支付凭证来生成。

[0162] 在步骤607中，移动支付应用程序123将支付信息(经加密的或不)发送到远程交易应用程序124。远程交易应用程序124接收经加密的或未加密的支付信息，如果没有加密，则加密支付信息，并生成包括经加密的支付信息的支付请求，与商家计算机130相关联的商家证书，以及未包括在经加密的支付信息内的与支付交易相关联的任何其他交易数据(例如，交易金额、商家标识符、产品标识符，等等)。

[0163] 如果支付信息还未加密，则远程交易应用程序124使用与远程密钥管理器140相关联的加密密钥来加密支付信息。例如，在一些实施例中，远程交易应用程序124可以使用一个或多个密钥，与远程密钥管理器140建立安全信道，以将敏感信息安全地传递到远程密钥管理器140。例如，远程交易应用程序124可以从移动支付应用程序123接收用来加密支付信息的密钥，以便创建与远程密钥管理器140的安全信道。另外，在一些实施例中，远程交易应用程序124可以存储远程密钥管理器加密密钥，并可以使用远程密钥管理器加密密钥来加密支付信息以及支付请求中的任何其他信息。

[0164] 在步骤608中，远程交易应用程序124可以将包括经加密的支付信息、商家证书，以及任何交易信息的支付请求传输到远程密钥管理器140。经加密的支付信息可包括其中包括用户认证数据(例如，PIN、口令，等等)以及由移动支付应用程序生成的安全值的安全信息。虽然在图6中未示出，但是，在一些实施例中，远程交易应用程序124可以发起并生成与远程密钥管理器140的安全信道，并可以使用与安全信道相关联的会话密钥，以将支付请求

传递到远程密钥管理器140。在这样的实施例中，可以使用与可以在远程密钥管理器140和通信设备的安全元件之间共享(例如，通过远程交易应用程序124或移动支付应用程序123)的主衍生密钥相关联的会话衍生密钥来建立安全信道。在这样的实施例中，会话密钥可以被用来发送支付请求以及从远程密钥管理器140接收支付响应。

[0165] 相应地，通信设备(例如，移动设备120)可以将包括用于验证与交易相关联的用户的用户认证数据(例如，口令、PIN，等等)、用于验证与交易相关联的设备的安全值(例如，移动支付应用程序密码)，以及用于处理远程交易的安全支付凭证和/或交易数据的安全通信发送到被配置成在单一步骤中为远程支付交易完成对于用户和设备两者的与账户发行方相关联的认证过程以及在认证之后确定与商家相关联的用于处理交易的安全密钥的单一实体。这是有利的，因为通常这样的认证过程要求多个单独的过程，并重定向到认证计算机，用于在通信设备和认证计算机或发行方系统之间的直接通信。相应地，远程密钥管理器提供用于对由通信设备发起的远程交易的认证和安全处理的简单并且有效率的集成点。

[0166] 在步骤609中，远程密钥管理器140的交易处理模块141(C)接收支付请求，并使用存储在远程密钥管理器140的私钥数据库141(G)中的对应的加密密钥(例如，私钥、对应的对称密钥、会话密钥，等等)，解密经加密的支付信息。相应地，远程密钥管理器服务器计算机可以使用与用于加密通信设备上的经加密的支付信息的第一加密密钥(例如，远程密钥管理器公钥)相关联的第二加密密钥(例如，远程密钥管理器私钥)来解密经加密的支付信息。相应地，远程密钥管理器140可以获取经解密的安全信息，其中包括用户认证数据(例如，PIN、口令，等等)和由移动支付应用程序123为远程交易生成的安全值(例如，密码)以及支付凭证，交易信息，等等。

[0167] 存储在私钥数据库141(G)上的远程密钥管理器私钥可包括任何合适的加密密钥，包括，例如，对称的加密密钥或公钥/私钥对的私钥。在使用远程密钥管理器私钥的各实施例中，私钥被配置成解密利用对应的远程密钥管理器公钥加密的信息，远程密钥管理器私钥安全地存储在远程密钥管理器140上，以使得远程密钥管理器140可以能够解密利用远程密钥管理器公钥加密的信息。类似地，远程密钥管理器对称密钥可以存储在远程密钥管理器140中，并用于解密经加密的支付信息。

[0168] 远程密钥管理器140的证书确认模块141(A)也可以通过应用存储在证书颁发机构公共根密钥数据库141(H)中的证书颁发机构根公钥，以验证公钥证书(例如，商家证书)是合法的并由合适的证书颁发机构180签名，验证在支付请求中接收到的验证商家证书是真实的。证书确认模块141(A)可以提取包括在商家证书中的商家公钥，以用于进一步处理远程交易。

[0169] 进一步，在其中在商家应用程序121中接收到的交易数据由商家计算机130签名的各实施例中，远程密钥管理器140可以通过检查以确保正确的商家公钥用于加密交易信息(例如，商家公钥与接收到的商家证书相关联)，支付信息的各方面是正确的(例如，商家标识符与已注册的商家相关联)，验证接收到的支付请求，并可以执行可以确保包括经加密的支付信息的支付请求正在由合法的支付应用程序、商家计算机130、商家应用程序121、通信设备(例如，移动设备120)等等发送的任何其他合适的验证。

[0170] 例如，在一些实施例中，远程密钥管理器140可以验证任何交易数据上的签名(如果由商家计算机130或对应的交易处理器利用接收到的公钥证书签名)。通常，可以通过从

该商家证书中提取商家计算机，使用商家证书中所包括的公钥来验证签名。可另选地，在一些实施例中，公钥可以是注册的并与商家证书相关联地存储在远程密钥管理器140中。如果签名未被验证，那么远程密钥管理器140向商家应用程序121指出签名无效，并且该方法停止。要注意，商家计算机130对交易信息进行签名以及由远程密钥管理器140验证签名是可选的并且可以根本不发生或可以周期性地发生，如此可以不从商家计算机130传递签名。

[0171] 在步骤610中，远程密钥管理器140安全信息验证模块141(D)可以通过利用认证计算机191发起认证过程，获取用于远程交易的认证响应值。如上文所描述的，远程密钥管理器140的安全信息验证模块141(D)可以通过不同的方法获取认证响应值。例如，对于图6所示出的实施例，远程密钥管理器140的安全信息验证模块141(D)可以生成认证请求，并将其发送到支付处理网络160。认证请求可包括经解密的安全信息，其中包括用户认证数据(例如，PIN、口令、等等)和由移动支付应用程序为远程交易生成的安全值(例如，密码)以及支付凭证，交易信息，以及用于验证认证请求的任何其他相关信息。

[0172] 在一些实施例(未示出)中，远程密钥管理器140可以与支付处理网络160相关联或是支付处理网络160的一部分，并可以通过确定与经解密的支付信息相关联的认证计算机191，并将包括安全信息的认证请求直接发送到认证计算机，获取认证响应值。例如，远程密钥管理器140功能可以被嵌入到支付处理网络160中，远程密钥管理器140可以访问目录服务器数据库，无需将认证请求发送到支付处理网络160。然而，对于图6所示出的实施例，远程密钥管理器140可以将认证请求发送到支付处理网络160，以便认证与远程支付交易相关联的用户和设备。

[0173] 在步骤611中，支付处理网络160的安全信息验证模块161(D)接收认证请求消息，并确定与认证请求相关联的认证计算机191。取决于支付处理网络160的配置，支付处理网络160的安全信息验证模块161(D)可以通过多个不同的过程来确定与认证请求相关联的认证计算机191。例如，安全信息验证模块161(D)可以通过使用嵌入到支付处理网络160中的目录服务器功能，通过从目录服务器计算机190请求认证计算机191的身份，或通过经过目录服务器接口模块161(C)将认证请求转发到目录服务器，来直接确定认证计算机191。

[0174] 在图6中示出的实施例中，支付处理网络服务器计算机161的安全信息验证模块161(D)可以将认证请求传递到目录服务器计算机190，目录服务器计算机190可以确定与认证请求相关联的认证计算机191的身份，并将认证请求传递到认证计算机191。相应地，在步骤611中，支付处理网络可以将认证请求转发到目录服务器计算机190，用于为认证请求确定和标识认证计算机191。相应地，支付处理网络服务器计算机161可以将经解密的安全信息发送到目录服务器计算机190，经解密的安全信息包括用户认证数据(例如，PIN、口令等等)和由移动支付应用程序为远程交易生成的安全值(例如，密码)以及支付凭证、交易信息以及用于验证认证请求的任何其他相关信息。

[0175] 然而，在其他实施例(未示出)中，支付处理网络服务器计算机161可以包括目录服务器计算机190的功能，如此可以直接确定认证计算机191。相应地，支付处理网络160的安全信息验证模块161(D)可以确定与认证请求相关联的认证计算机191的身份，此后，支付处理网络计算机161可以将认证请求转发到认证计算机191。支付处理网络160的安全信息验证模块161(D)可以通过确定与认证请求相关联的账户发行方，搜索发行方认证配置数据库161(E)以查找与账户发行方相关联的认证计算机191，确定认证计算机191的身份，此后，支

付处理网络计算机161可以将认证请求转发到认证计算机191。

[0176] 例如，认证请求可包括经解密的支付信息，其中包括与远程支付应用程序相关联的账户标识符(例如，PAN)。支付处理网络160的安全信息验证模块161(D)可以确定与账户信息相关联的账户发行方(例如，通过从账户标识符(例如，PAN)中提取发行方标识符(例如，BIN))，并搜索账户发行方认证配置数据库161(E)，以查找被配置成处理与确定的发行方相关联的认证请求和/或与账户信息相关联的确定的账户范围(例如，与不同类型账户或账户范围相关联的不同的认证计算机的发行方的，等等)的认证计算机191。

[0177] 进一步地，在一些实施例中，可以针对单一认证请求，标识一个以上的认证计算机191。例如，可以标识与支付处理网络160相关联的第一认证计算机191，用于对由移动支付应用程序123生成的安全值的“代表”认证，而可以标识与账户发行方相关联的第二认证计算机191，用于对用户认证数据的验证。相应地，安全信息验证模块161(D)可以将认证请求发送到被配置成完成对每一特定类型的安全信息的认证的两个认证计算机。

[0178] 相应地，支付处理网络160的安全信息验证模块161(D)可以通过搜索发行方共享的秘密数据库161(F)，以查找与发行方、账户，或用于生成安全值的移动支付应用程序123相关联的共享的秘密，代表账户发行方执行安全值认证。共享的秘密可包括算法、查询表，或由账户发行方在通信设备的安全元件122上提供账户的过程中所提供的与账户、设备，和/或移动支付应用程序123相关联的任何其他信息。另选地或另外地，可以由账户发行方提供主共享的秘密密钥，该主共享的秘密密钥可以被用来为与发行方相关联的每一个账户，生成衍生共享的秘密密钥。不管怎样，支付处理网络160的安全信息验证模块161(D)都可以检索与认证请求相关联的合适的共享的秘密，确定该认证请求的安全值，并将确定的安全值与接收到的安全值进行比较，以将移动支付应用程序123验证为可靠的且经确认的。

[0179] 取决于与认证请求相关联的共享的秘密的类型，可通过任何合适的方法来确定安全值。例如，在安全值是动态的情况下，安全信息验证模块161(D)可以从发行方共享的秘密数据库161(F)中检索共享的秘密算法，并向共享的秘密算法应用从认证请求接收到的输入数据。例如，可以将PAN的最后四位、到期数据、以及现时值(nonce)(即，从移动支付应用程序123接收到的不可预测的值)应用于确定的共享的秘密算法，以便生成认证请求的安全值。

[0180] 在安全值是静态的各实施例中，安全信息验证模块161(D)可以在发行方共享的秘密数据库161(F)中搜索与账户、发行方、移动支付应用程序123、用户相关联的静态共享的秘密，或与共享的秘密数据库相关联的任何其他变量。例如，如果共享的秘密是静态卡确认值(CVV)，则安全信息验证模块可以在发行方共享的秘密数据库161(F)中搜索与PAN相关联的条目，并且可以确定与颁发的卡和/或账户相关联的静态CVV。因此，支付处理网络160或认证计算机191可以使用任何合适的方法来确定并验证安全值。

[0181] 然而，如图1所示，在一些实施例中，支付处理网络160可以将认证请求转发到目录服务器，该目录服务器可以确定与认证请求相关联的相关认证计算机191。可另选地，支付处理网络160可以从目录服务器计算机190请求认证计算机191的身份，然后，将认证请求发送到认证计算机191。目录服务器计算机190可以执行与上文对于标识与认证请求相关联的认证计算机191所描述的过程类似的过程。

[0182] 在步骤612中，目录服务器计算机190可以接收包括经解密的安全信息的认证请

求。经解密的安全信息可包括用户认证数据(例如,PIN、口令、等等)和由移动支付应用程序为远程交易生成的安全值(例如,密码)以及支付凭证,交易信息,以及用于验证认证请求的任何其他相关信息。目录服务器计算机190可以通过上文参考支付处理网络160所描述的相同过程,确定与认证请求相关联的认证计算机,包括,例如,确定与认证请求中的支付凭证相关联的发行方标识符(例如,BIN),并搜索发行方认证配置数据库或包括认证计算机地址以及与确定的发行方标识符(例如,BIN)相关联的认证计算机191的账户发行方关联的任何其他数据库。

[0183] 一旦目录服务器计算机190确定了与认证请求相关联的认证计算机191,目录服务器计算机190就可以将认证请求转发到确定的认证计算机191。要注意,可以通过经加密的通信信道接收并发送从支付处理网络服务器计算机161接收到的认证请求并转发到认证计算机191的认证请求,以便认证请求和包括的安全信息被保护,并防止被恶意的第三方截取。可以使用任何合适的加密密钥,加密和解密加密过程中的(例如,步骤610-616)中的各种实体之间的每一通信,以便每一步骤中的加密过程都被防止截取。

[0184] 在步骤613中,认证计算机191可以接收包括安全信息的认证请求,并可以验证安全信息并生成包括认证响应值的认证响应。如上文所描述的,认证计算机191可以由账户发行方、由代表账户发行方的支付处理网络160,或由第三方系统操作。

[0185] 认证计算机191可以通过对照存储在认证数据库中的用户认证数据和安全验证信息验证由用户输入的用户认证数据和/或由支付应用程序(例如,移动支付应用程序123)生成的安全值来验证认证请求中的安全信息。例如,认证数据库可以存储提供给通信设备的移动支付应用程序123的共享的秘密以及由账户发行方在注册过程中或用户的其他账户确认过程中存储的用户认证数据。

[0186] 认证计算机191可以通过与上文针对支付处理网络服务器计算机的对安全值的验证所描述的过程相同的过程来验证安全值。因此,认证数据库可以存储共享的秘密算法、查询表或可以被用来确定账户的安全值的任何其他可确认的信息,并将确定的安全值与认证请求中的接收到的安全值进行比较。如果安全值相同,则认证请求可以被验证为来源于真正的通信设备、移动支付应用程序123,和/或远程交易应用程序124。

[0187] 例如,验证安全值(例如,密码)可以由支付处理网络160使用在认证请求中接收到的交易信息和/或支付信息来生成。如果接收到的密码匹配生成的验证密码,则认证计算机191可以确认支付信息是由有效并且可靠的移动支付应用程序123生成的。

[0188] 类似于安全值验证,认证计算机191可以验证用户认证数据(例如,PIN、口令,等等)。因此,认证数据库可以存储将与消费者账户相关联的用户认证数据(例如,PIN、口令,等等),用户认证数据可以被用来确定账户的存储的用户认证数据,并可以将确定的用户认证数据与认证请求中的接收到的用户认证数据进行比较。如果认证数据相同或在合理的阈值内匹配,则认证请求可以被验证为与被授权的用户或账户持有人相关联,或是被授权的用户或账户持有人发起的。

[0189] 例如,用户认证输入(例如,口令)可以由用户在远程支付交易的发起过程中输入。口令可以在经加密的支付信息中被传递到远程密钥管理器140,经加密的支付信息可在通过支付处理网络160发送到与用户的账户的账户发行方相关联的认证计算机191的认证请求中包括用户认证数据(例如,口令)。认证计算机191可以查找存储在与用户的账户相关联

的认证数据库中的已存储的用户认证数据(例如,口令),并可以比较并验证存储的用户认证数据(例如,口令)匹配接收到的用户认证数据(例如,口令)。

[0190] 可另选地或组合地,认证计算机191可以确定移动支付应用程序123、远程交易应用程序124、支付处理网络160,和/或其他受信任的实体是否预先认证了消费者110,并可以使用此信息来判断是否执行消费者认证过程以及认证请求是否被认证。例如,在一些实施例中,发行方可以将与消费者账户相关联的共享的秘密信息提供到安全元件122中的个性化的移动支付应用程序123或远程交易应用程序124。因此,移动支付应用程序123或远程交易应用程序124可以对照供应的用户认证数据(例如,口令)来验证接收到的用户认证数据(例如,口令)并确定用户是否是可靠的。如果用户认证数据匹配(如此,消费者被认证),那么认证的结果(例如,认证的用户)可被提供在生成并发送到远程密钥管理器140的支付请求中并且随后被包括在转发到认证计算机191的认证请求中。

[0191] 因此,认证计算机191可以确定用户是否被预先认证,被什么实体或应用程序,是否可以执行附加的认证,认证计算机191可以控制与认证请求相关联的认证决策。因此,在一些实施例中,包括在发起交易之前由移动支付应用程序123或远程交易应用程序124执行的持卡人确认方法的安全信息可以被传递到支付处理网络计算机161、目录服务器计算机190,以及认证计算机191,并且被用于认证远程交易。

[0192] 另外,还可以使用任意数量的内部或外部认证过程,进一步认证认证请求。例如,可以完成基于风险的、存储的凭证、质询-响应,或任何其他类型的消费者认证过程。在一些实施例中,远程密钥管理器140可以通过认证请求、质询,对密码的请求,或通过任何其他合适的方法,从消费者110请求认证信息。

[0193] 如果认证过程成功且安全信息被验证,则认证计算机191可以使用与账户发行方计算机170和/或支付处理网络160相关联的共享的秘密认证响应算法来生成交易的认证响应值(例如,验证密码)。可以由账户发行方计算机170或支付处理网络160在授权过程中验证认证响应值,以便通过指出交易被预先分析并被认证计算机191认证来提供交易的附加级别的认证。另外,可以在认证响应中改变或提供安全级别指示符,该安全级别指示符向交易处理生态系统内的其他实体指出,使用两因素用户和设备安全信息,认证了交易。安全级别指示符可以允许交易中的其他实体以任意数量的不同的方式,改变它们的行为,并可以向其他实体指出,哪一方承担交易的责任(例如,支付处理网络,而不是商家,等等)。

[0194] 在步骤614中,认证计算机191可以生成包括认证响应值、提高的安全级别指示符和/或认证处理器的成功的指示的认证响应,并将其返回到目录服务器计算机190或支付处理网络160(取决于系统的配置)。可另选地,如果认证过程不成功,则可以返回错误或其他拒绝并且交易可以停止。

[0195] 在步骤615中,目录服务器计算机190可以接收认证响应,并将认证响应转发到支付处理网络服务器计算机。认证响应可包括认证响应值,安全级别指示符,以及成功的指示(以及安全信息、交易信息、支付凭证,等等中的任何一项)。要注意,通信在每一实体之间可被加密以确保安全性和端对端加密过程。

[0196] 在步骤616中,支付处理网络服务器计算机161可以接收认证响应消息,确定与认证响应消息相关联的远程密钥管理器140,并将认证响应消息发送到远程密钥管理器140。认证响应可包括认证响应值,安全级别指示符,以及成功的指示(以及安全信息、交易信息、

支付凭证，等等中的任何一项)。要注意，通信在每一实体之间可被加密以确保安全性和端对端加密过程。

[0197] 在步骤617中，远程密钥管理器140可以从支付处理网络160接收认证响应，并可以确定认证过程的结果。因此，如果认证过程成功并且远程密钥管理器140接收到认证响应，该认证响应包括指出由与账户发行方和/或支付处理网络160相关联的认证计算机191对安全信息的验证的认证响应值(例如，验证密码)，远程密钥管理器140可以继续远程交易处理。

[0198] 因此，远程密钥管理器140可以更新经解密的支付信息以包括认证响应值、安全性指标以及来自认证响应的任何其他验证信息。在一些实施例中，安全信息可以被替换为认证响应值和/或安全性指标。在其他实施例中，认证响应值和安全性指标可以附加到或添加到经解密的支付信息。

[0199] 如果远程密钥管理器140尚未提取商家公钥，则远程密钥管理器140的公钥提取模块141(B)可以从商家证书(或其他交易处理器证书)中提取公钥。然后，远程密钥管理器140的交易处理模块141(C)可以使用确定的商家公钥，重新加密支付信息。如上所述，商家公钥可以被包括在商家应用程序证书中，并在远程交易处理过程中的任何一点被提取。远程密钥管理器140可以以任何合适的方式确定商家公钥，包括从商家证书中提取公钥，使用向远程密钥管理器140注册的商家的存储的商家公钥，或通过任何其他合适的方式。

[0200] 在步骤618中，远程密钥管理器140的交易处理模块141(C)生成支付响应，其中包括经重新加密的支付信息，并将其发送到通信设备(例如，移动设备120)。可以通过预先用于接收支付请求的安全信道发送支付响应，或可以通过开放信道将经加密的支付信息发送到移动设备120的远程交易应用程序124。因此，在一些实施例中，可以使用为远程密钥管理器140和移动设备120之间的安全通信预先建立的会话密钥，进一步加密经重新加密的支付信息。

[0201] 在步骤619中，远程交易应用程序124接收经重新加密的交易响应，并将交易响应中的经重新加密的支付信息转发到商家应用程序121。可以使用任意数量的不同的方法来将经重新加密的支付信息发送到商家计算机130。例如，支付响应消息可包括与商家计算机130相关联的未加密的路由信息，以便商家应用程序121可以自动地将经重新加密的支付信息路由到商家计算机130。另选地或另外地，商家应用程序121可以具有被编程到商家应用程序121中的与商家计算机130相关联的路由信息(例如，服务器计算机地址)，当发起交易时，商家应用程序121可以知道，任何相应的支付响应消息可以被路由到商家计算机130。进一步，包括经重新加密的支付信息的接收到的消息中的标志或其他数据元素可以向商家应用程序121指出向哪里以及在哪个实体中发送经重新加密的支付信息。

[0202] 另外，在一些实施例中，远程密钥管理器140可以被配置成直接将支付响应发送到商家计算机130。因此，远程密钥管理器140可以使用包含在商家证书中的地址信息，在远程支付处理服务的注册过程中提供的商家信息，或在购物请求中提供的商家信息，以确定要直接发送购买响应的合适的商家服务器计算机。

[0203] 在步骤620中，商家应用程序121将经重新加密的支付信息发送到商家计算机130。商家应用程序121可以通过任何合适的方法，确定用于发送经重新加密的支付信息的合适的商家计算机130。例如，路由信息可以被包括在支付响应中，当支付被发起时，商家应用程

序121可以具有与远程支付交易相关联的目的地商家计算机130，或商家应用程序121可以具有要发送支付响应的指定的商家计算机130。

[0204] 在步骤621中，商家计算机130接收经重新加密的支付信息，并使用存储在商家计算机130上的商家私钥，解密经重新加密的支付信息。如此，在远程交易处理中的第一时间，商家计算机130可以访问移动支付应用程序123从移动通信设备的安全存储器中获取的且加密的支付信息(例如，支付凭证和/或包括认证响应值的其他安全信息)。例如，商家服务器可以获取与支出账户相关联的账户标识符(例如，主账户号码(PAN))和到期日期，以及交易特定的安全值和认证响应值。认证响应值(例如，卡认证确认值(CAVV))为支付处理器和/或发行方提供附加认证和验证机会，并实现最小化远程交易中的诈骗风险。因此，商家服务器计算机现在具有安全支付凭证、认证响应值(例如，CAVV)、安全级别指示符和/或责任指示符，交易信息，以及用于发起支付交易的任何其他相关信息。

[0205] 相应地，商家计算机130可以使用经解密的支付信息来发起和/或执行支付交易。例如，商家计算机130可以生成授权请求消息，其包括通常将存在于“卡存在”交易中的信息(例如，支付凭证，安全值，等等)，以及添加了指出消费者110预先被认证可进行交易的认证响应值。相应地，商家计算机130可以将经解密的支付信息(以及支付响应中所包括的其他交易信息)映射到与商家计算机130、收单方计算机150、支付处理网络160，以及发行方计算机170的授权请求消息相关联的格式。

[0206] 在步骤622中，商家计算机130可以通过将授权请求消息发送到与商家计算机130相关联的收单方计算机150，发起支付交易。认证请求消息可以具有被映射到授权请求消息内的预定的字段的经解密的支付信息，以便允许交易生态系统内的交易实体(例如，收单方计算机150、支付处理网络160、发行方计算机170，等等)标识与交易相关联的支付凭证(例如，账户)和认证级别并处理交易。

[0207] 在步骤623中，收单方计算机150可以将授权请求消息路由到与提供在授权请求消息中的发行方标识符(例如，BIN)或账户标识符(例如，主要账户标识符)相关联的支付处理网络160。

[0208] 在步骤624中，支付处理网络160可以接收授权请求消息，并可以验证授权请求消息中的认证响应值。支付处理网络160可以解析授权请求消息，以确定认证响应值，并可以访问可以被用来验证在认证请求消息中接收到的认证响应值的认证响应共享的秘密算法或其他加密密钥。例如，认证响应值共享的秘密算法可包括用于生成认证响应值以便生成验证认证值的远程密钥管理器密钥、账户发行方密钥，或支付处理网络密钥。如果验证认证值和认证响应值匹配，则支付处理网络160可以知道交易被预先认证并确定此交易是欺骗性的可能性低。相应地，交易可以立即被授权或可以向发行方提供附加的认证信息以通知它们交易可能的是可靠的并应该被授权。

[0209] 另选地或另外地，通过与上述类似的验证过程，可以由发行方计算机170使用发行方共享的秘密密钥来认证认证响应值，该发行方共享的秘密密钥被认证计算机191用来生成该认证响应值。因此，在支付交易的发起之后并且在支付交易的处理期间，认证响应值可以由支付处理网络160或账户发行方计算机170来验证。

[0210] 在步骤625中，支付处理网络160将授权请求消息转发到与消费者账户相关联的发行方计算机170。

[0211] 在步骤626中，发行方计算机170可以执行风险评估和授权决策过程，其中，发行方计算机170可以从授权请求消息解析相关信息，该授权请求消息包括认证响应值、来自与交易相关的支付处理网络160的任何验证信息(例如，风险分数、其他认证过程的结果，等等)，并且发行方计算机170可以作出关于交易是否被授权的决定。

[0212] 在步骤627中，然后，发行方计算机170可以生成授权响应消息(包括交易是否被授权的指示)，并将其通过支付网络返回，最终(虽然未示出)返回到商家计算机130和消费者110(通过移动设备120)以指示交易是否被授权以及是否成功地完成。

[0213] 应该理解，图6只是描述性的而非限制性的。例如，可以使用任意数量的不同的实体来解密经重新加密的支付信息(例如，移动网关、移动钱包提供商、支付处理网络，等等)。另外，其他交易处理实体(例如，商家应用程序121、收单方计算机150、支付服务提供商，等等)也可以被配置成解密经重新加密的支付信息并发起支付交易。

[0214] II.附加的实施例

[0215] 另外，虽然图6示出了商家计算机130通过解密经重新加密的支付信息并将经解密的支付信息映射到授权请求消息来发起支付交易，但是可以基于与远程支付交易相关联的交易处理器的身份来完成使用远程密钥管理器140和移动设备120的商家应用程序121进行远程交易的附加示例性方法。例如，可以使用交易处理器证书来确定与解密经重新加密的支付信息并发起远程交易相关联的交易处理器。例如，远程密钥管理器140可以使用与多个不同的交易处理实体(例如，商家应用程序121、商家计算机130、收单方计算机150、支付服务提供商(PSP)，等等)相关联的公钥来重新加密支付信息。因此，取决于在交易处理以及系统的配置期间传递的证书，交易处理器可以变化。

[0216] 例如，代替使用商家公钥来加密支付信息，商家应用程序公钥(与存储在商家应用程序121上的私钥相关联的)或收单方公钥(与存储在收单方计算机中的私钥相关联的)可以被用来加密支付信息，可以将经重新加密的支付信息传递到每一相应的实体(例如，商家服务器计算机或收单方计算机150)，用于解密和授权请求消息生成。相应地，取决于远程交易处理系统的配置，在一些实施例中，可以将任意数量的公钥证书(例如，商家应用程序公钥证书、商家公钥证书、收单方公钥证书，等等)传递到远程密钥管理器140。一旦从远程密钥管理器140返回经重新加密的支付信息，商家应用程序121就可以确定应该提供哪一个公钥证书以及经加密的支付信息的路由信息。

[0217] 相应地，交易处理器证书的身份可包括商家应用程序121、商家计算机130，或收单方计算机150中的任何一个。因此，远程密钥管理器140可以利用从接收到的公钥证书中提取的公钥来验证接收到的公钥证书，解密经加密的支付信息(例如，账户标识符和密码)，并重新加密经解密的支付信息(例如，卡数据和密码)。如上所述，公钥证书可以与任何交易处理器相关联，例如包括，商家计算机130、商家应用程序121、或收单方计算机150。此后，远程密钥管理器140可以将经重新加密的支付信息发送到与接收到的公钥证书(以及随后用于加密支付信息的公钥)相关联的交易处理实体(例如，商家应用程序121、商家计算机130、收单方计算机150，等等)。

[0218] 例如，在第一实施例中，公钥证书可包括商家应用程序公钥证书，如此远程密钥管理器140验证证书并提取或以别的方式获取商家应用程序公钥。因此，商家应用程序公钥用于重新加密经解密的支付信息，并且远程密钥管理器140将经重新加密的支付信息发送到

商家应用程序121。商家应用程序121可以接收经重新加密的支付信息，确定与经重新加密的支付信息相关联的商家应用程序私钥，并使用商家应用程序私钥来解密经重新加密的支付信息。相应地，商家应用程序121可以具有存储在安全元件122上的敏感信息以及使用移动支付应用程序123的用于支付交易的安全算法生成的安全信息。

[0219] 然后，商家应用程序121可以使用经解密的支付信息来发起支付交易。商家应用程序121可以使用任何合适的方法来发起支付交易。例如，商家应用程序121可以生成配置成通过支付处理网络160发送的授权请求消息。可另选地，虽然在图6中未示出，但是商家应用程序121可以使用商家服务器密钥，再次加密经解密的支付信息，并可以将支付信息发送到商家计算机130，以便解密并发起支付交易。如此，可以将经解密的支付信息传递到商家计算机130，以用于授权请求消息的生成或支付交易的其他发起。可以将类似的过程应用于任何其他交易处理器(例如，收单方计算机、支付服务提供商系统，等等)。

[0220] 另外，在一些实施例中，远程密钥管理器可包括至支付处理网络160的移动网关，支付处理网络160可以执行上文所描述的远程密钥管理器140和支付处理网络160的全部功能。因此，移动设备120可以将支付请求的经加密的支付信息直接传递到配置成处理远程支付交易的支付处理网络160。因此，用于在移动支付应用程序123和远程密钥管理器140之间进行通信的远程密钥管理器140和加密密钥可以与支付处理网络160相关联。

[0221] 移动网关(未示出)可包括安全信道生成模块，该安全信道生成模块配置成在移动网关、移动设备120，以及支付处理网络计算机161之间配置安全通信链路。安全信道生成模块可以交换任何相关信息，以便移动支付应用程序123和移动网关生成用于安全地传递敏感信息的匹配的或互补的会话密钥。可以实施用于生成安全信道的任何其他合适的方法。

[0222] 可在2012年10月29日提交的名为“Over The Air Update of Payment Transaction Data Stored in Secure Memory(储存在安全存储器中的支付交易数据的空中更新)”美国专利No.13/662,843、2009年9月21日提交的名为“Apparatus and Method for Preventing Unauthorized Access to Payment Application Installed in Contactless Payment Device(防止对安装在免接触支付设备中的支付应用的未授权访问的装置和方法)”的美国专利申请No.12/563,410以及2009年9月21日提交的名为“Over The Air Update of Payment Transaction Data Stored in Secure Memory(储存在安全存储器中的支付交易数据的空中更新)”的美国专利申请No.13/563,421中找到关于移动网关190的能力的进一步信息，这些申请出于所有目的引用其整体结合于此。

[0223] 在带有移动网关的各实施例中，可以建立安全信道，并可以在移动支付应用程序123、与支付处理网络160相关联的移动网关，以及支付处理网络计算机161之间发送通信，以便初始化并准备安全信道。安全信道允许移动设备120和支付处理网络160之间的未来通信被加密并防止被截取。

[0224] 安全信道可以以任何合适的方式来建立。例如，可以使用在移动支付应用程序123的个性化过程中提供到移动支付应用程序123中的移动网关加密密钥，建立安全信道。相应地，用于建立安全信道的加密密钥可包括每一会话或远程支付交易都改变的会话密钥。在2011年3月30日提交的授予Aabye等人的美国专利申请No.13/075,592中描述了类似的过程，这里引用了该申请作为参考。

[0225] 进一步，加密密钥可以是从由移动支付应用程序123发行方，与安全元件122相关

联的受信任的服务管理器(TSM)，或安全元件发行方所提供的主密钥衍生唯一衍生密钥(UDK)。另外，如那些精通相关技术的人所认识的，可以实现任何其他合适的加密方法。如此，可以使用数据加密标准，诸如，例如，带有至少124位的密钥的RSA、三重数据加密标准(DES)、128位高级加密标准(AES)、使用最小128位密钥长度的RC4流加密算法，等等来实现安全连接。

[0226] 在建立安全信道之后，移动支付应用程序123可以使用存储在安全元件122中的支付凭证和存储的或使用存储在安全元件122中的信息衍生的移动网关加密密钥(例如，共享的加密密钥或用于为每一个会话生成唯一衍生密钥的方式)来生成并发送包含经加密的支付信息的支付请求。因此，移动网关可以解密由移动支付应用程序123提供的经加密的支付信息，而不会影响从商家服务器传递的并利用支付处理网络公钥加密的经加密的交易信息。因此，移动网关可以使用一个加密密钥以用于安全信道上的通信，支付处理网络160可以使用不同的加密密钥以用于解密由商家计算机130提供的经加密的交易信息。因此，移动支付应用程序123可以使用第一密钥(例如，会话密钥)来生成并安全地传递存储在移动设备120的安全元件122中的支付凭证和消费者信息，而支付处理网络160可以使用第二密钥(例如，支付处理网络私钥)来解密从商家服务器计算机传递的交易信息。

[0227] 另外，在一些实施例中，可以在支付处理网络160上实现令牌注册表或令牌保险库，以使得支付处理网络160能够使作为认证请求的一部分接收到的令牌去令牌化，以确定用于认证远程交易的账户和对应的账户发行方，如上文所描述的。因此，支付处理网络160也可以通信地耦合到令牌注册表或与令牌注册表合并，该令牌注册表可包括任何数据库或其他存储器，其中令牌可以被发行到通信设备并与发行方账户相关联的以使得可以使用令牌代替主账户号码/标识符(PAN)来处理交易。

[0228] 另外，在一些实施例中，远程密钥管理器140可包括第三方服务提供商系统(例如，移动钱包提供商)。例如，第三方服务器提供商可包括与消费者110、移动设备120、商家、支付处理网络160，或任何其他支付交易处理方法或系统具有利益或关系的任何实体。例如，第三方服务提供商系统可以包括移动钱包提供商、移动设备制造商、移动网络运营商，或可以与商家和消费者设备连接的任何其他实体。相应地，本发明的各实施例可以允许第三方服务提供商系统注册商家并管理商家远程交易的认证过程，以提供对远程交易的更安全的处理。

[0229] 最后，虽然各实施例专注于远程支付交易，但是，各实施例不限于这样的交易，此处所描述的认证概念可以用于许多不同类型的交易。例如，各实施例可以被用来认证并授权供应过程、卡或账户确认/验证过程和/或任何其他发行方或其他服务提供商过程，其中当使用通信设备时认证可能是有帮助的。

[0230] 如此，通过远程密钥管理器140传递的认证请求和响应消息可以被用来从相关服务提供商或利益方获取针对任何相关活动的认证。例如，在用户供应过程的情况下，在通信设备上供应账户之前，本文所描述的认证过程和系统可以被用来认证用户的了解您的客户(KYC)信息(例如，社会保障号码、出生日期、邮政编码、等等)或任何其他个人信息，以允许发行方在供应过程期间认证消费者110或账户。因此，在移动设备中供应账户期间，消费者110可以向远程交易应用程序124输入他们的用户认证数据，个人信息、对提示问题的回答或任何其他相关信息连同他们的账户凭证(例如，PAN、到期日期，等等)，以便发起账户信息

在通信上的供应，并从与账户的发行方相关联的认证计算机191获取授权。

[0231] 这样的认证和验证过程可以使用账户供应请求来实现，以与图6在上面示出的过程类似，该账户供应请求可以允许消费者110请求利用与使用远程密钥管理器140的账户发行方相关联的特定账户信息来个性化移动支付应用程序123。

[0232] 例如，远程交易应用程序124、移动支付应用程序123、远程密钥管理器140、支付处理网络160、目录服务器计算机190以及认证计算机191之间的交互可以与图6所示出的相同。然而，代替传递与远程支付交易相关联的经加密的支付信息，消费者110可以输入并传递与账户相关联的经加密的个人信息和支付凭证，以允许发行方：标识该账户；将消费者110认证为与关于消费者110的已知信息(例如，账户持有人的KYC信息)相关联；以及作出关于供应过程的授权决定，以及提供账户供应响应，账户供应响应允许供应系统发起账户信息的供应。

[0233] 账户供应响应可包括可以被供应系统用来在通信设备上供应账户的任何信息。例如，账户供应响应可包括供应响应值(或任何其他指示符)，该供应响应值为供应系统提供授权以在通信设备上供应账户。另外，账户供应响应可包括可以被用来在通信设备上供应账户的经生成的账户供应脚本或其他格式化的信息和/或指令。相应地，供应脚本可以被传送到与发行方、认证计算机191、支付处理网络160、通信设备，或远程交易处理系统中的任何其他实体相关联的供应系统或受信任的服务管理器，以便在通信设备上供应账户。

[0234] 另外，账户供应响应可包括可以在上文所描述的远程支付交易处理期间使用的用户认证数据(例如，PIN、口令、密码，等等)。相应地，可以使用认证基础结构来建立要结合支付交易一起使用的用户认证数据。在一些实施例中，可以在账户供应响应中返回用户认证数据，该账户供应响应通过上文的图6的步骤613-618所示的认证系统而发回。在一些实施例中，可以在账户供应响应之外通过另一信道或通过另一已知通信方法(例如，电子邮件、SMS，等等)来传递用户认证数据以确保消费者110通过第二或单独的通信方法获取用户认证数据。通过确保消费者110可以访问现有的通信方法以获取用户认证数据，可以进一步保证系统安全。

[0235] 因此，在一些实施例中，消费者110可以将个人信息输入到远程交易应用程序124、移动支付应用程序123或任何其他移动设备中，以便在经由远程密钥管理器140提供给认证计算机191的供应请求期间认证他们本身。移动应用程序或远程交易应用程序124可以连同账户凭证一起将传递到移动支付应用程序123，该移动支付应用程序123可以使用存储的加密密钥来加密个人信息，如上所述。然后，移动支付应用程序123可以将经加密的个人信息传递到远程交易应用程序124，以便发送到远程密钥管理器140。远程密钥管理器140可以解密个人信息和/或账户信息，并发起如参考图6的步骤610-616所描述的认证过程。

[0236] 例如，可以使用供应请求中所包括的账户凭证/信息来标识认证计算机191，认证计算机191可以将个人信息与已注册的与账户相关联的消费者信息进行比较，以验证消费者110。例如，社会保障号码、地址、出生日期，或任何其他信息可以由消费者110提供，并作为供应请求验证的一部分来验证。在验证消费者110之后，认证计算机191可以生成脚本或以别的方式返回账户供应响应消息，该消息指出供应系统可以在通信设备上供应账户信息。

[0237] 因此，可以在远程支付交易之外提供由本发明的各实施例所提供的优点，这些优

点可以允许针对通信设备的有效率的认证过程以与用于任何类型的认证过程的认证系统连接。

[0238] III.示例性计算机设备

[0239] 图7是可以被用来实现上文所描述的实体或部件中的任何一个的计算机系统的高级别框图。图7所示出的子系统经由系统总线775互连。附加的子系统包括打印机703、键盘706、固定盘707,以及耦合到显示适配器704的监视器709。耦合到I/O控制器700的外围设备以及输入/输出(I/O)设备可以通过本领域内已知的任意数量的装置(诸如串行端口)连接到计算机系统。例如,串行端口705或外部接口708可以被用来将计算机设备连接到诸如因特网之类的广域网,鼠标输入设备,或扫描仪。通过系统总线775的互连允许中央处理器702与每一子系统进行通信并控制来自系统存储器701或固定盘707指令的执行,以及子系统之间的信息交换。系统存储器701和/或固定盘可以具体化计算机可读取的介质。

[0240] 用于包含代码或代码的多个部分的存储介质和计算机可读介质可包括本领域中已知或已使用的任何合适的介质,包括存储介质和通信介质,诸如但不仅限于以任何方法或技术实现的用于诸如计算机可读指令、数据结构、程序模块或其他数据之类的信息的存储和/或传输的易失性和非易失性、可移动和不可移动介质,包括RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光存储设备、磁带盒、磁带、磁盘存储设备或其他磁存储设备、数据信号、数据传输,或可用于存储或传输期望的信息并可由计算机访问的任何其他介质。基于本文中提供的公开和教导,本领域普通技术人员将理解实现各实施例的其他方式和/或方法。

[0241] 上文的描述仅是说明性的,而不是限制性的。在本领域技术人员阅读了本公开之后,本发明的许多变体对于他们会变得显而易见。因此,可不参考以上描述来确定本发明的范围,相反,可以参考待审查的权利要求书以及它们的完整范围或等效方案来确定本发明的范围。

[0242] 可以理解,能以模块或集成的方式、使用计算机软件、以控制逻辑的形式来实现上文所述的本发明。基于本文中提供的公开和教导,本领域普通技术人员可以知晓并理解使用硬件以及硬件和软件的组合来实现本发明的其他方式和/或方法。

[0243] 本申请中所描述的软件部件或功能中的任何一个都可以实现为软件代码,处理器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(诸如例如,Java、C++或Perl)来执行的这些软件代码。软件代码可以作为一系列指令或命令被存储在计算机可读介质上,计算机可读介质诸如,随机存取存储器(RAM)、只读存储器(ROM)、诸如硬驱动器或软盘之类的磁介质,或诸如CD-ROM之类的光介质。任何此类计算机可读介质都可以驻留在单个的计算装置上或单个的计算装置内,并可以存在于系统或网络内的不同的计算装置上或不同的计算装置内。

[0244] 来自任何实施例的一个或多个特征可以与任何其他实施例的一个或多个特征相结合而不背离本发明的范围。

[0245] 对“一”(“a”、“an”)或“所述”(“the”)的引用旨在是指“一个或多个”,除非特别指示为相反的情况。

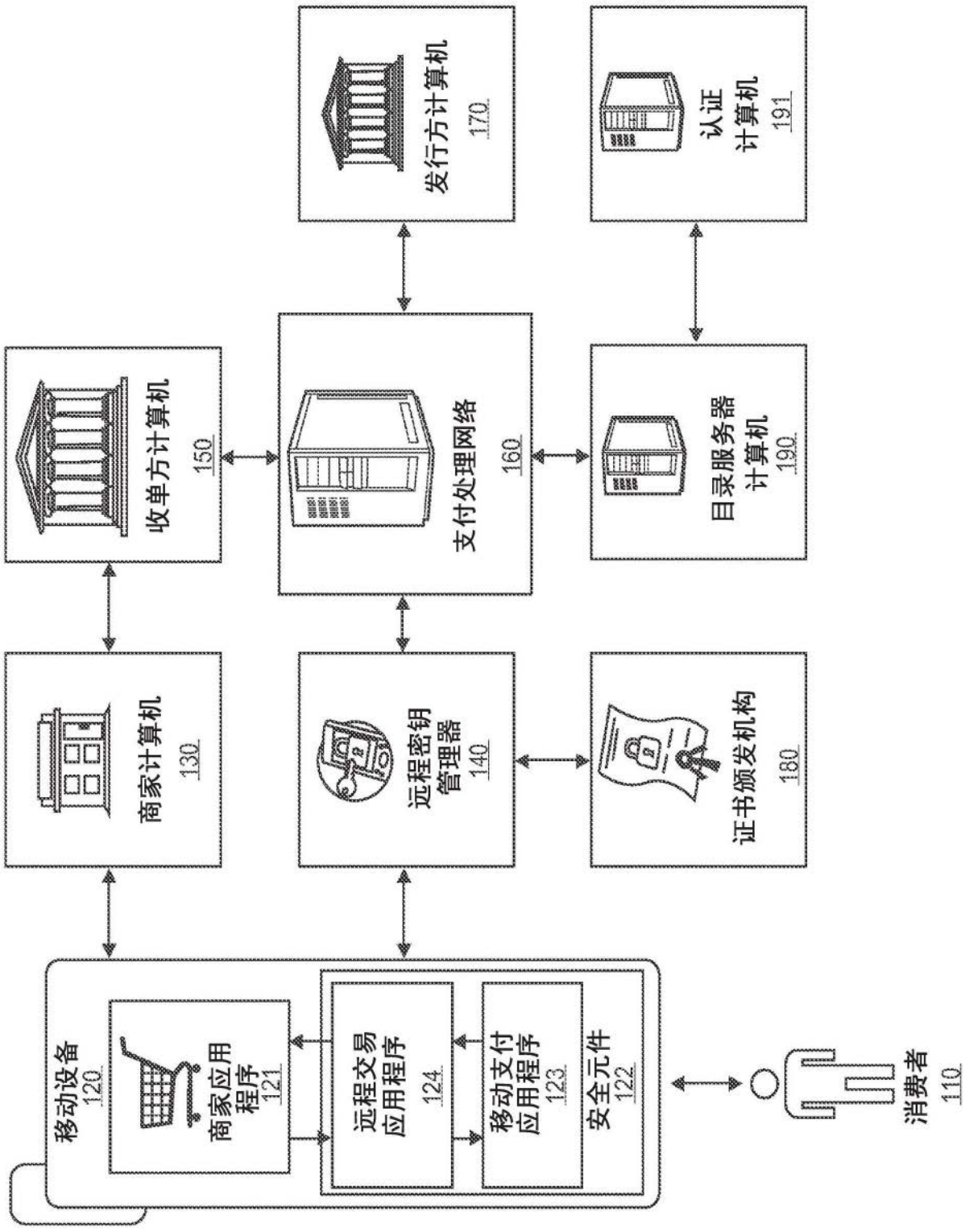

发行方计算机
170
认证
计算机
191
收单方计算机
150
支付处理网络
160
目录服务器
计算机
190
商家计算机
130
远程密钥
管理器
140
证书颁发机构
180
移动设备
120
商家应用
程序
121
远程交易
应用程序
124
移动支付
应用程序
123
安全元件
122
消费者
110

图1

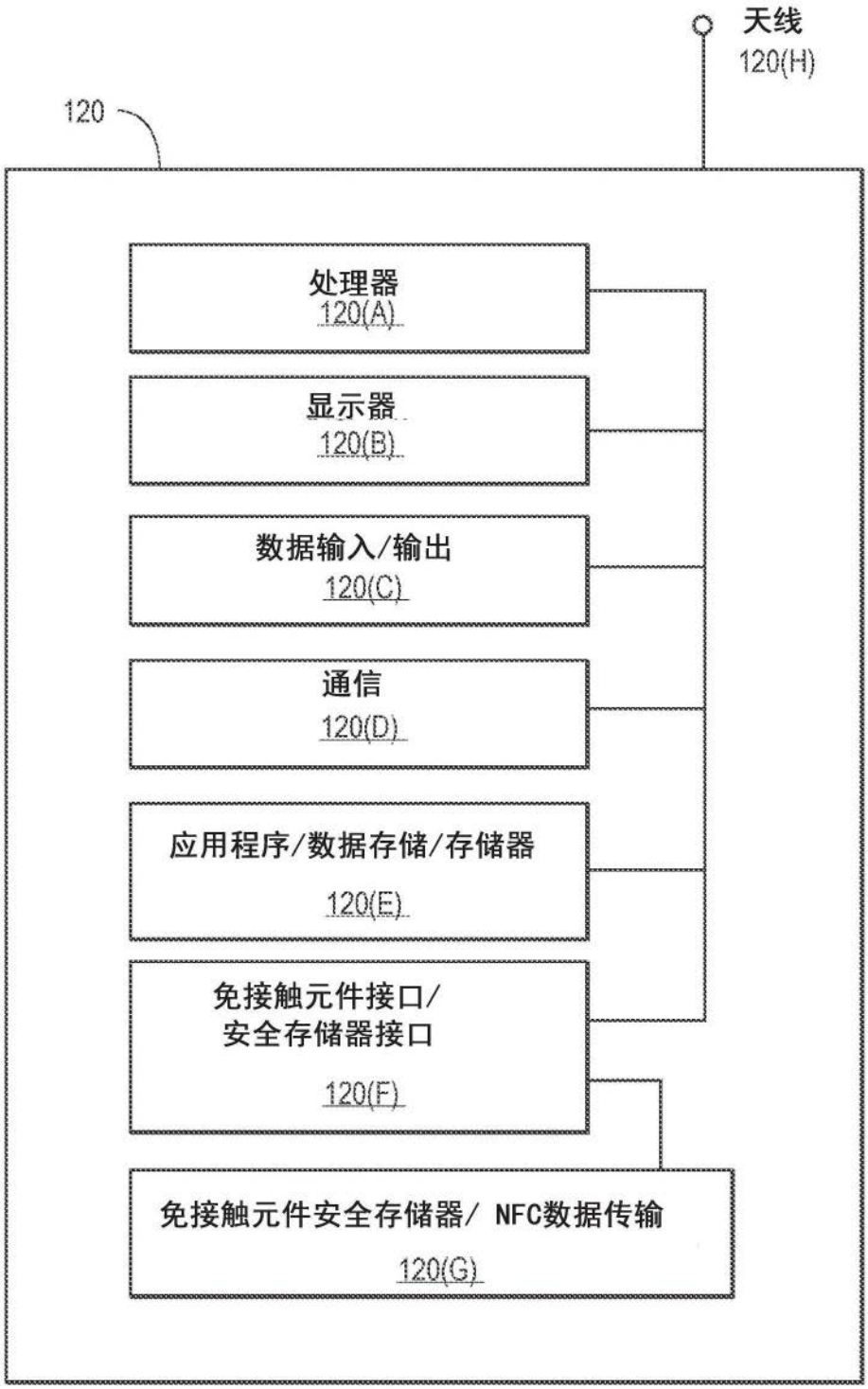

天线
120(H)
120
处理器
120(A)
显示器
120(B)
数据输入/输出
120(C)
通信
120(D)
应用程序/数据存储/存储器
120(E)
免接触元件接口/
安全存储器接口
120(F)
免接触元件安全存储器/ NFC数据传输
120(G)

图2

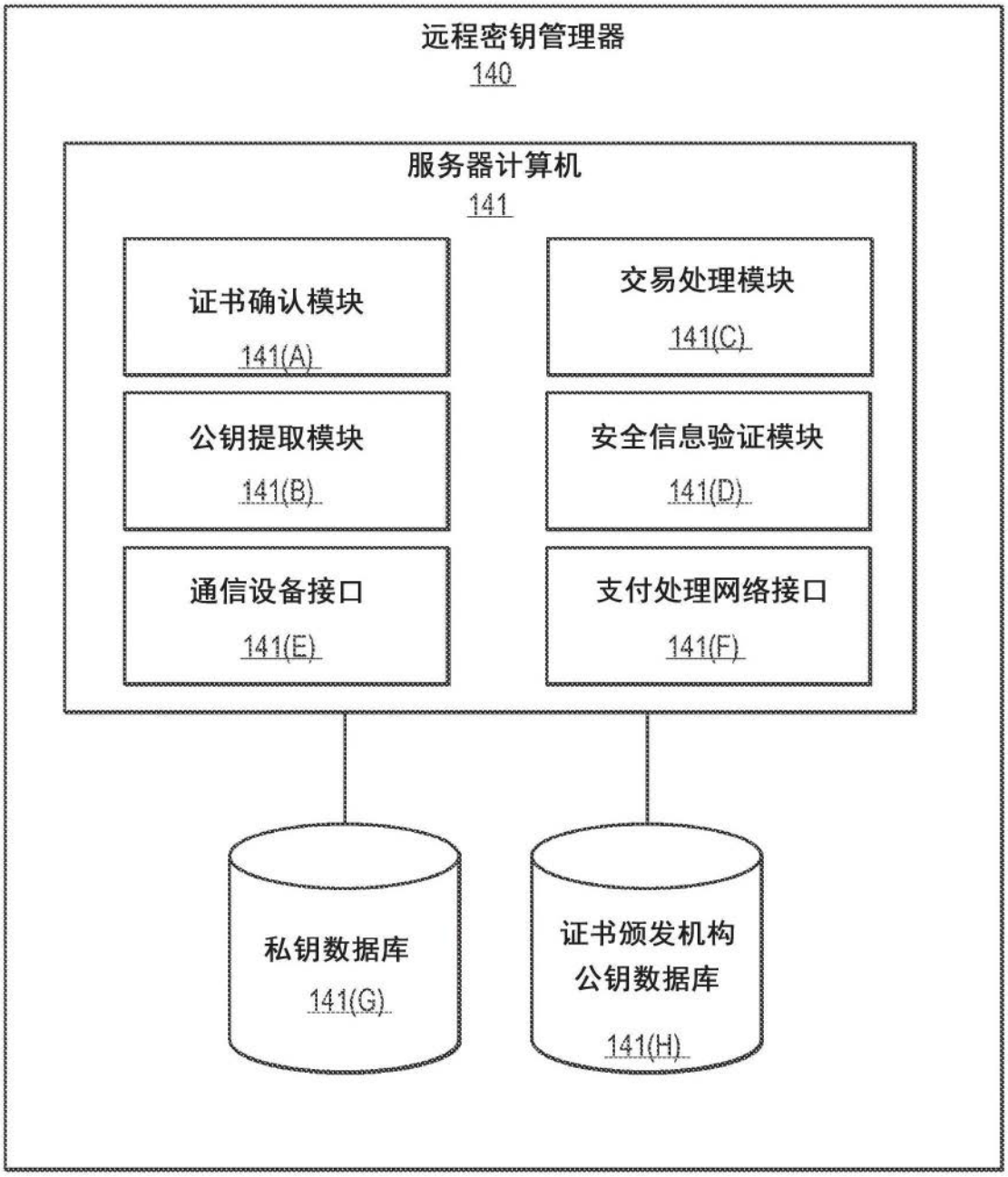

远程密钥管理器
140
服务器计算机
141
证书确认模块
141(A)
交易处理模块
141(C)
公钥提取模块
141(B)
安全信息验证模块
141(D)
通信设备接口
141(E)
支付处理网络接口
141(F)
私钥数据库
141(G)
证书颁发机构
公钥数据库
141(H)

图3

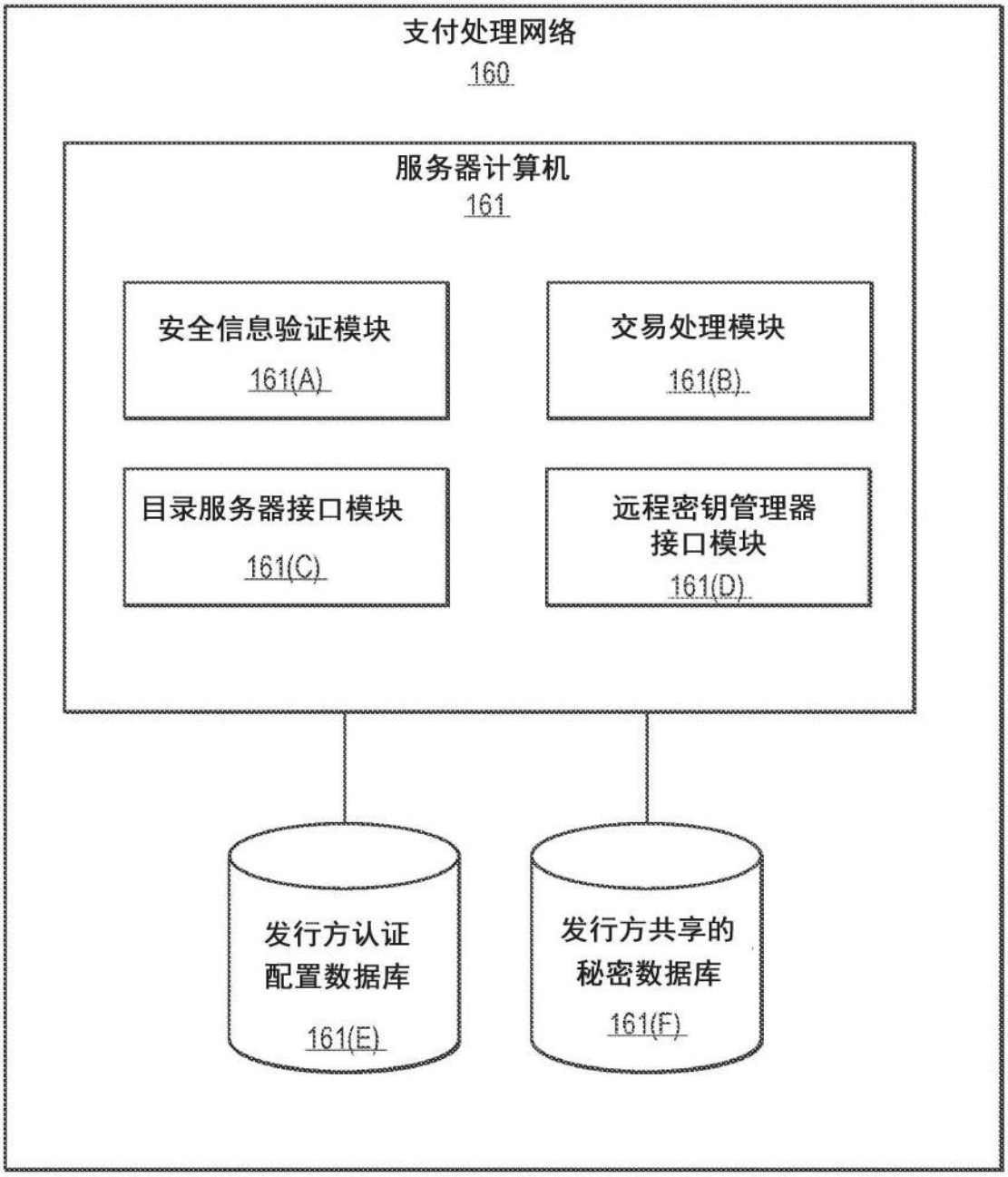

支付处理网络
160
服务器计算机
161
安全信息验证模块
161(A)
交易处理模块
161(B)
目录服务器接口模块
161(C)
远程密钥管理器
接口模块
161(D)
发行方认证
配置数据库
161(E)
发行方共享的
秘密数据库
161(F)

图4

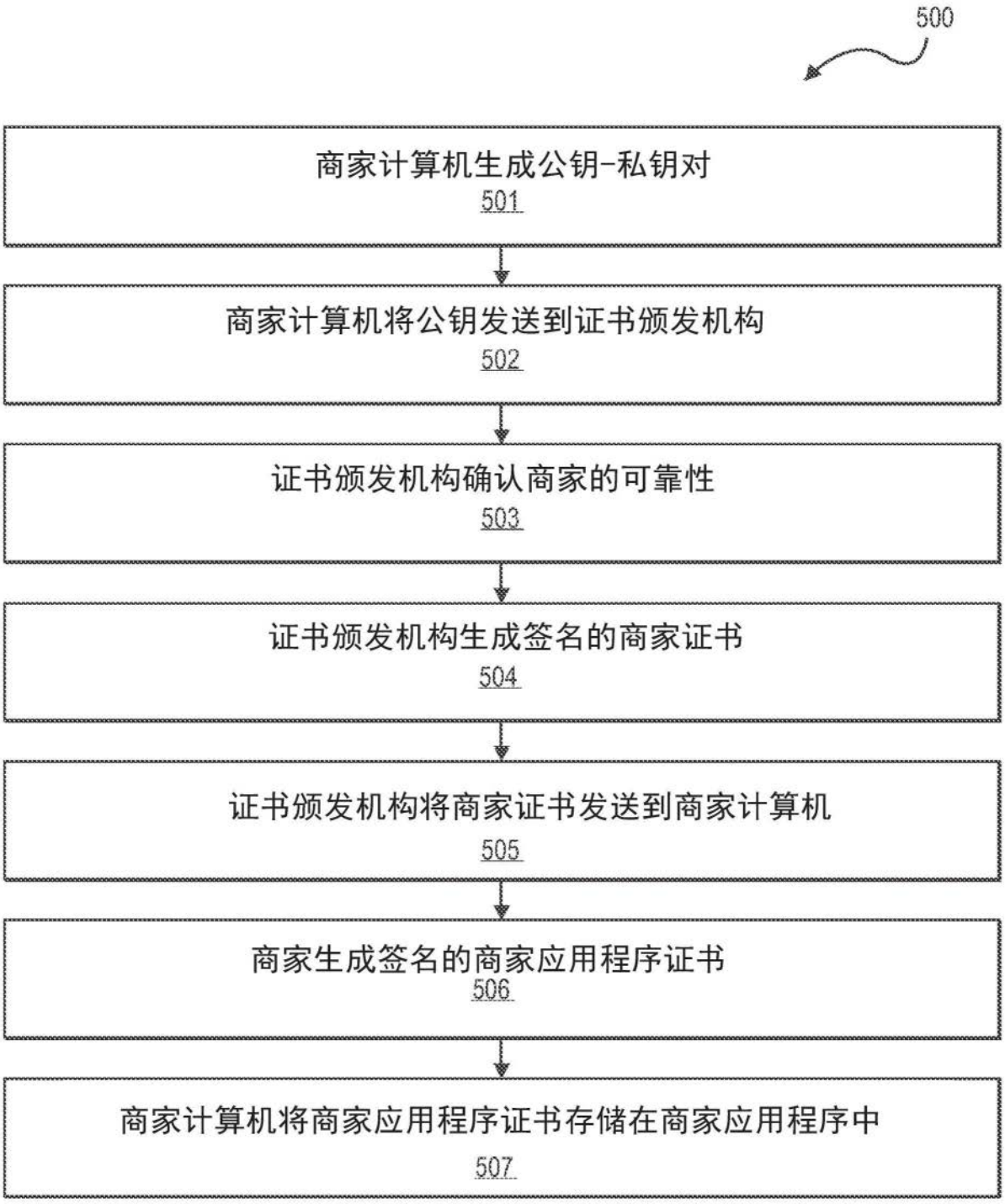

500
商家计算机生成公钥-私钥对
501
商家计算机将公钥发送到证书颁发机构
502
证书颁发机构确认商家的可靠性
503
证书颁发机构生成签名的商家证书
504
证书颁发机构将商家证书发送到商家计算机
505
商家生成签名的商家应用程序证书
506
商家计算机将商家应用程序证书存储在商家应用程序中
507

图5

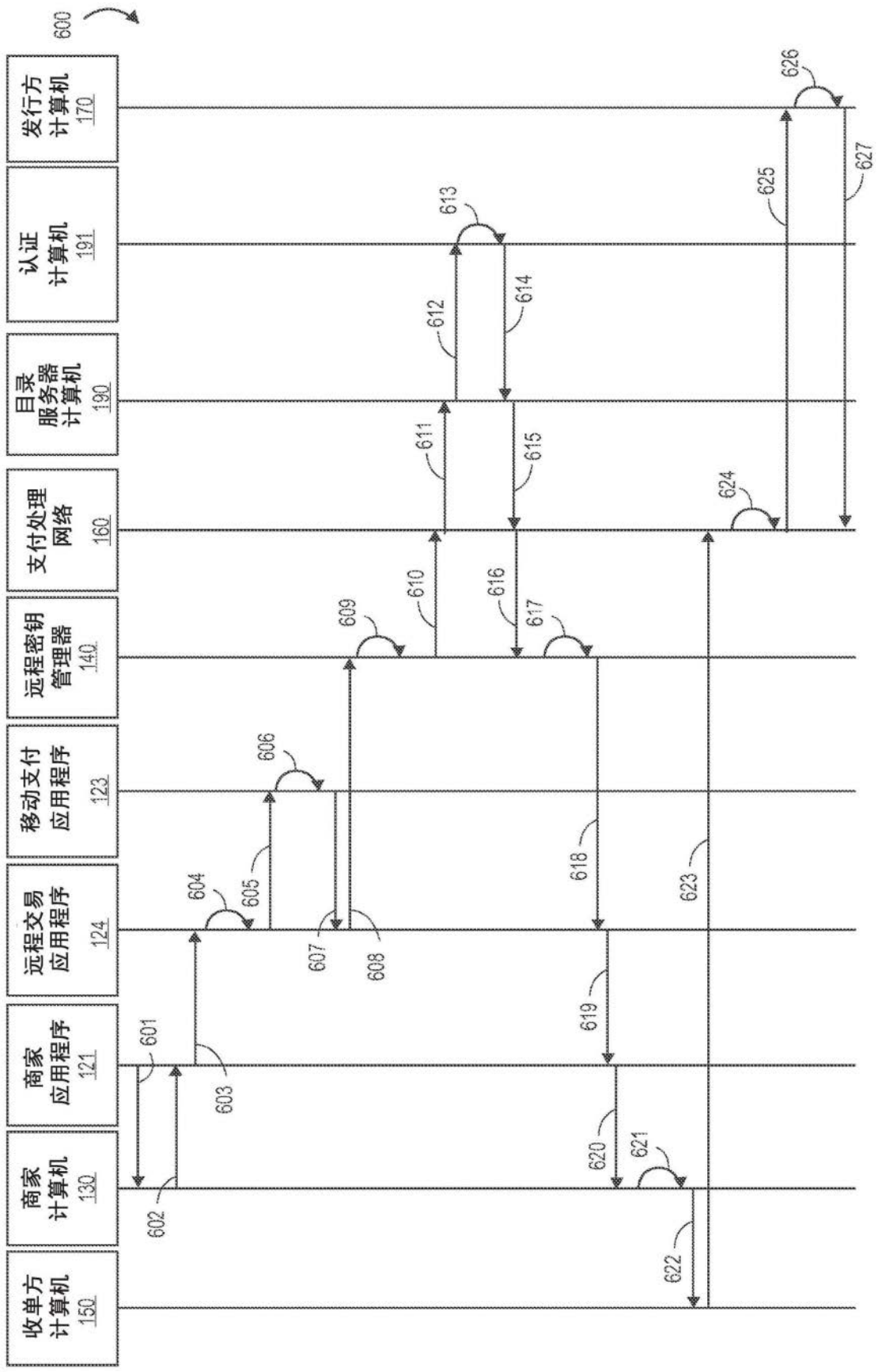

600
发行方计算机 170
认证计算机 191
目录服务器计算机 190
支付处理网络 160
远程密钥管理器 140
移动支付应用程序 123
远程交易应用程序 124
商家应用程序 121
商家计算机 130
收单方计算机 150
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627

图6

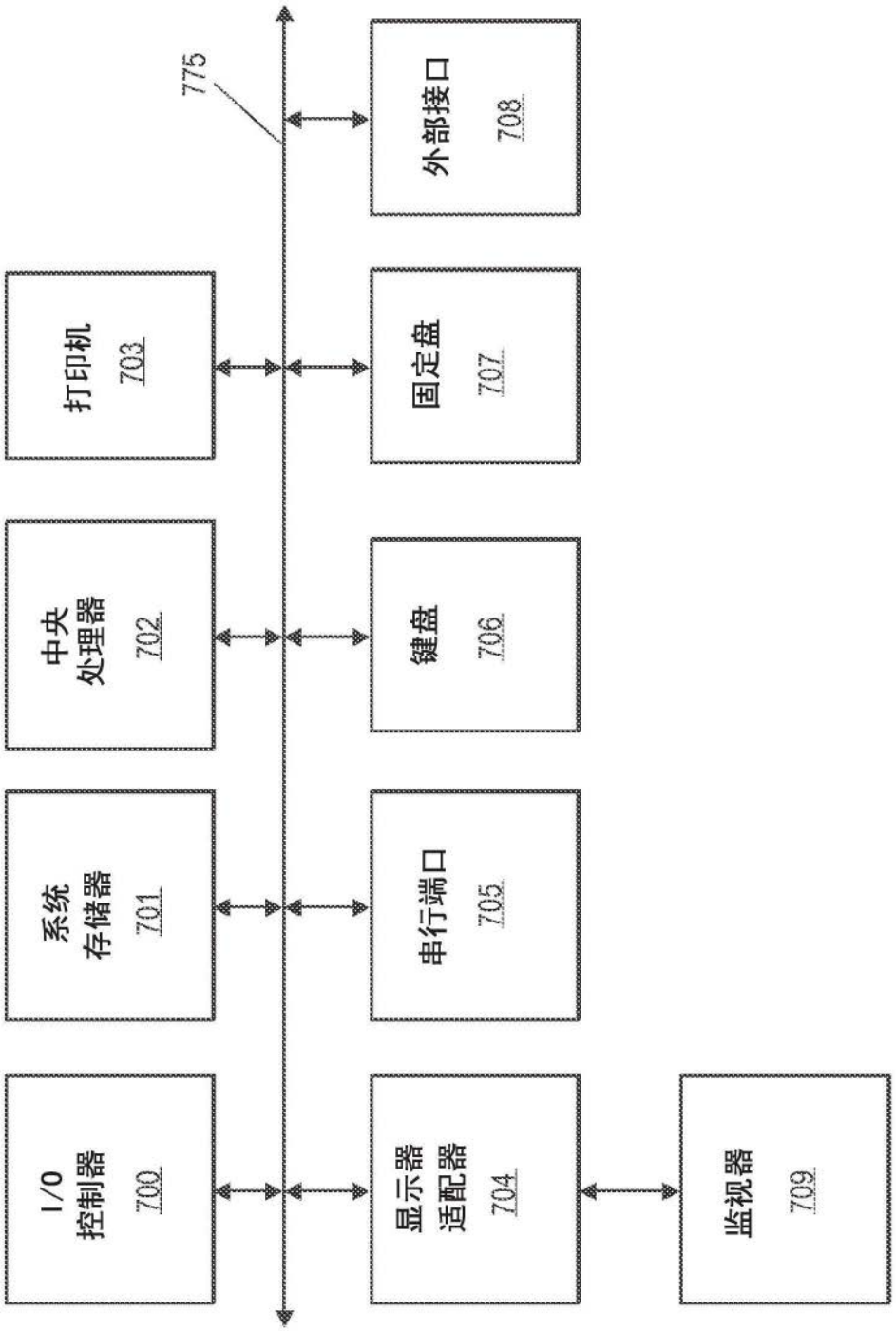

775
外部接口
708
打印机
703
固定盘
707
中央
处理器
702
键盘
706
系统
存储器
701
串行端口
705
I/O
控制器
700
显示器
适配器
704
监视器
709

图7