(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106664556 A
(43)申请公布日 2017.05.10

(21)申请号 201580044386.9

(22)申请日 2015.08.12

(30)优先权数据
14/463,276 2014.08.19 US

(85)PCT国际申请进入国家阶段日
2017.02.17

(86)PCT国际申请的申请数据
PCT/US2015/044894 2015.08.12

(87)PCT国际申请的公布数据
WO2016/028572 EN 2016.02.25

(71)申请人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 O·J·贝诺伊特
P·丁娜功西素帕普

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
G06Q 20/20(2012.01)
G06Q 20/32(2012.01)
G06Q 20/40(2012.01)
H04L 29/06(2006.01)

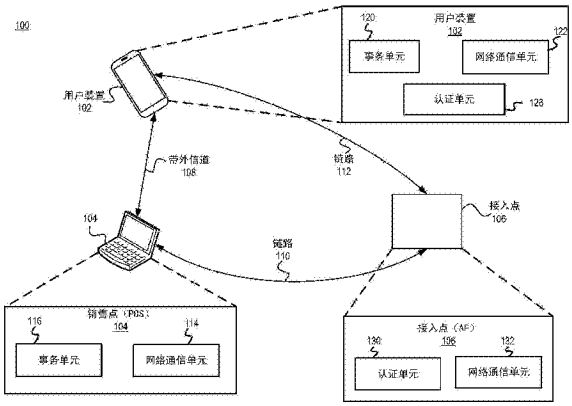
权利要求书4页 说明书13页 附图7页

(54)发明名称

利用销售点装置进行网络接入认证

(57)摘要

可以配置用户装置(102)进行网络接入，例如用于访客网络接入。在一个范例中，第一装置(104)接收使用所述第一装置(102)的事务的指示。第一装置(102)响应于接收到所述事务的指示，向网络的接入点(106)传送对网络接入的请求。第一装置(104)然后从接入点(106)接收第一密钥。第一装置(104)向用户装置(102)提供第一密钥。用户装置(102)是使用第一密钥来获得对网络的网络接入的。



CN 106664556 A

1.一种用于网络接入的方法,包括:

在网络的第一装置处接收使用所述第一装置的事务的指示;

响应于接收到所述事务的指示,向所述网络的接入点传送对网络接入的请求;

从所述接入点接收第一密钥;以及

向用户装置提供所述第一密钥,其中

所述用户装置是使用所述第一密钥来获得所述网络接入的。

2.根据权利要求1所述的方法,其中,

所述用户装置与所述接入点通信,以至少部分地基于所述第一密钥来产生第二密钥,并且

所述用户装置进一步与所述接入点通信,以进一步基于所述第二密钥来获得对所述网络的接入。

3.根据权利要求2所述的方法,其中,

所述第一密钥是非对称密钥,并且

所述第二密钥是对称密钥。

4.根据权利要求2所述的方法,其中,所述第二密钥包括以下密钥之一:

成对主密钥(PMK),

成对临时密钥(PTK),或

预共享密钥(PSK)。

5.根据权利要求1所述的方法,其中,

所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

6.根据权利要求5所述的方法,其中,所述OOB信道包括包含了以下各项的组中的至少一个成员:

光信道,

近场通信(NFC)信道,

蜂窝信道,以及

蓝牙信道。

7.根据权利要求1所述的方法,其中,

所述接入点产生包括所述第一密钥和第二密钥的第一密钥对,

所述第一密钥为公共密钥,并且所述第二密钥为私有密钥,

所述用户装置产生包括第三密钥和第四密钥的第二密钥对,

所述第三密钥为公共密钥,并且所述第四密钥为私有密钥,并且

所述用户装置与所述接入点通信,以基于所述第一密钥对和所述第二密钥对来获得所述网络接入。

8.根据权利要求1所述的方法,其中,

所述事务在所述用户装置和所述第一装置之间。

9.根据权利要求1所述的方法,其中,

在所述第一密钥被提供给所述用户装置时,由所述接入点产生的所述第一密钥的格式是被保持的。

10.根据权利要求1所述的方法,其中,

所述接入点是响应于接收到对所述网络接入的所述请求，来产生所述第一密钥的，并且

所述第一密钥是对称密钥。

11.根据权利要求1所述的方法，其中，

所述用户装置进一步与所述接入点通信，以至少部分地基于所述第一密钥来获得所述网络接入。

12.一种计算装置，包括：

处理器；以及

其中存储有程序指令的存储器，所述程序指令可以由所述处理器执行以使得所述计算装置执行以下步骤，

接收使用所述计算装置的事务的指示；

响应于接收到所述事务的指示，向网络的接入点传送对网络接入的请求；

从所述接入点接收第一密钥；以及

向用户装置提供所述第一密钥，其中

所述用户装置是使用所述第一密钥来获得所述网络接入的。

13.根据权利要求12所述的计算装置，其中，

所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥来产生第二密钥，并且

所述用户装置进一步与所述接入点通信，以进一步基于所述第二密钥来获得对所述网络的接入。

14.根据权利要求13所述的计算装置，其中，

所述第一密钥是非对称密钥，并且

所述第二密钥是对称密钥。

15.根据权利要求13所述的计算装置，其中，所述第二密钥包括以下密钥之一：

成对主钥匙(PMK)，

成对临时密钥(PTK)，或者

预共享密钥(PSK)。

16.根据权利要求12所述的计算装置，其中，

所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

17.根据权利要求12所述的计算装置，其中，

所述接入点产生包括所述第一密钥和第二密钥的第一密钥对，

所述第一密钥为公共密钥，并且所述第二密钥为私有密钥，

所述用户装置产生包括第三密钥和第四密钥的第二密钥对，

所述第三密钥为公共密钥，并且所述第四密钥为私有密钥，并且

所述用户装置与所述接入点通信，以基于所述第一密钥对和所述第二密钥对来获得所述网络接入。

18.根据权利要求12所述的计算装置，其中，

所述事务在所述用户装置和所述第一装置之间。

19.根据权利要求12所述的计算装置，其中，

在所述第一密钥被提供给所述用户装置时，由所述接入点产生的所述第一密钥的格式是被保持的。

20.根据权利要求12所述的计算装置，其中，

所述接入点是响应于接收到对所述网络接入的所述请求，来产生所述第一密钥的，并且

所述第一密钥是对称密钥。

21.一种用于网络接入的方法，包括：

由网络的第一装置向所述网络的接入点传送对网络接入的请求；

在所述第一装置处从所述接入点接收第一密钥；

处理与用户装置的支付事务，其中

处理所述支付事务包括，

向所述用户装置提供所述第一密钥，并且

从所述用户装置接收第二密钥，并且

所述用户装置是使用所述第一密钥来获得所述网络接入的；以及向所述接入点提供所述第二密钥。

22.根据权利要求21所述的方法，其中，

所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥和所述第二密钥来产生第三密钥，并且

所述用户装置进一步与所述接入点通信，以进一步基于所述第三密钥来获得所述网络接入。

23.根据权利要求21所述的方法，其中，

处理所述支付事务还包括从所述用户装置接收支付数据。

24.根据权利要求21所述的方法，其中，

所述接入点是在处理所述支付事务之前产生所述第一密钥的。

25.根据权利要求22所述的方法，其中，

所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

26.一种计算装置，包括：

处理器；以及

其中存储有程序指令的存储器，所述程序指令可以由所述处理器执行以使得所述计算装置执行以下步骤，

向网络的接入点传送对网络接入的请求；

从所述接入点接收第一密钥；

处理与用户装置的支付事务，其中，

处理所述支付事务包括，

向所述用户装置提供所述第一密钥，以及

从所述用户装置接收第二密钥，并且

所述用户装置是使用所述第一密钥来获得所述网络接入的；以及向所述接入点提供所述第二密钥。

27.根据权利要求26所述的计算装置，其中，

所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥和所述第二密钥来产生第三密钥，并且

所述用户装置进一步与所述接入点通信，以进一步基于所述第三密钥来获得所述网络接入。

28.根据权利要求26所述的计算装置，其中，

处理所述支付事务还包括从所述用户装置接收支付数据。

29.根据权利要求26所述的计算装置，其中，

所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

30.根据权利要求26所述的计算装置，其中，

所述接入点是在处理所述支付事务之前产生所述第一密钥的。

利用销售点装置进行网络接入认证

[0001] 相关内容

[0002] 本申请要求享有2014年8月19日提交的美国申请No.14/463276的优先权。

技术领域

[0003] 本公开内容的实施例总体涉及通信系统领域，并且更具体而言，涉及配置通信装置以用于通信网络之内。

背景技术

[0004] 有时用户可能希望将计算装置连接到访客网络以获得对因特网和其他网络资源的接入。为了连接到访客网络，用户可以参与认证过程以使得用户的计算装置通过访客网络的接入点(AP)获得对可用的网络资源的接入。一种认证过程包括用户在用户的计算装置上输入密码。不过，用户在计算装置上输入密码通常很麻烦。此外，用户能够与他人共享密码，使得密码的安全性降低。

[0005] 另一种认证过程包括将用户计算装置上的浏览器重定向到用于认证的强制网络门户。不过，该过程可能导致在认证过程之前已经加载到浏览器中的针对网页的未定义的行为。为了避免未定义行为，用户通常必须记得在认证过程期间刷新或重新启动浏览器，以便在浏览器上加载强制网络门户。此外，可以通过分组嗅探器来利用强制网络门户。上述两种认证过程都依赖于口令进行用户认证。这些口令通常很弱，可能被敌对方猜测到。一旦知道了口令，敌对方就能够建立用于模仿合法AP的流氓AP，给用户带来安全威胁。

发明内容

[0006] 公开了配置用户装置进行网络接入，例如进行访客网络接入的各种实施例。在一个实施例中，第一装置接收使用所述第一装置的事务的指示。第一装置响应于接收到所述事务的指示，向网络的接入点传送对网络接入的请求。第一装置然后从接入点接收第一密钥。第一装置向用户装置提供第一密钥。用户装置是使用第一密钥来获得对网络的网络接入的。

[0007] 在另一实施例中，网络的第一装置向网络的接入点传送对网络接入的请求。该第一装置从接入点接收第一密钥。第一装置处理与用户装置的支付事务，包括向用户装置提供第一密钥，以及从用户装置接收第二密钥。用户装置是使用第一密钥来获得对所述网络的网络接入的。第一装置向接入点提供第二密钥。

[0008] 在一些实施例中，一种网络接入的方法包括：在网络的第一装置处接收使用所述第一装置的事务的指示；响应于接收到所述事务的指示，向所述网络的接入点传送对网络接入的请求；从所述接入点接收第一密钥；以及向用户装置提供第一密钥，其中，所述用户装置是使用所述第一密钥来获得所述网络接入的。

[0009] 在一些实施例中，所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥来产生第二密钥，并且所述用户装置进一步与所述接入点通信，以进一步基于所述第

二密钥来获得对所述网络的接入。

[0010] 在一些实施例中，第一密钥是非对称密钥，第二密钥是对称密钥。

[0011] 在一些实施例中，第二密钥包括如下之一：成对主密钥(PMK)、成对临时密钥(PTK)或预共享密钥(PSK)。

[0012] 在一些实施例中，所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

[0013] 在一些实施例中，该OOB信道包括由光信道、近场通信(NFC)信道、蜂窝信道和蓝牙信道构成的组中的至少一个成员。

[0014] 在一些实施例中，所述接入点产生包括所述第一密钥和第二密钥的第一密钥对，其中第一密钥为公共密钥，第二密钥为私有密钥；所述用户装置产生包括第三密钥和第四密钥的第二密钥对，其中第三密钥为公共密钥，第四密钥为私有密钥；并且所述用户装置与所述接入点通信，以基于所述第一密钥对和所述第二密钥对来获得所述网络接入。

[0015] 在一些实施例中，该事务在用户装置和第一装置之间。

[0016] 在一些实施例中，在所述第一密钥被提供给所述用户装置时，由所述接入点产生的所述第一密钥的格式是被保持的。

[0017] 在一些实施例中，所述接入点是响应于接收到对所述网络接入的请求来产生所述第一密钥的，并且第一密钥为对称密钥。

[0018] 在一些实施例中，所述用户装置进一步与所述接入点通信，以至少部分地基于所述第一密钥来获得所述网络接入。

[0019] 在一些实施例中，一种计算装置包括：处理器；以及其中存储有程序指令的存储器，所述程序指令可以由所述处理器执行以使得所述计算装置执行以下步骤：接收使用所述计算装置的事务的指示；响应于接收到所述事务的指示，向所述网络的接入点传送对网络接入的请求；从所述接入点接收第一密钥；以及向用户装置提供第一密钥，其中，所述用户装置是使用所述第一密钥来获得所述网络接入的。

[0020] 在一些实施例中，所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥来产生第二密钥，并且所述用户装置进一步与所述接入点通信，以进一步基于所述第二密钥来获得对所述网络的接入。

[0021] 在一些实施例中，第一密钥是非对称密钥，第二密钥是对称密钥。

[0022] 在一些实施例中，第二密钥包括如下之一：成对主密钥(PMK)、成对临时密钥(PTK)或预共享密钥(PSK)。

[0023] 在一些实施例中，所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

[0024] 在一些实施例中，所述接入点产生包括所述第一密钥和第二密钥的第一密钥对，其中第一密钥为公共密钥，第二密钥为私有密钥；所述用户装置产生包括第三密钥和第四密钥的第二密钥对，其中第三密钥为公共密钥，第四密钥为私有密钥；并且所述用户装置与所述接入点通信，以基于所述第一密钥对和所述第二密钥对来获得所述网络接入。

[0025] 在一些实施例中，该事务在用户装置和第一装置之间。

[0026] 在一些实施例中，在所述第一密钥被提供给所述用户装置时，由所述接入点产生的所述第一密钥的格式是被保持的。

[0027] 在一些实施例中，所述接入点是响应于接收到对所述网络接入的请求来产生所述第一密钥的，并且第一密钥为对称密钥。

[0028] 在一些实施例中，一种用于网络接入的方法包括：由网络的第一装置向所述网络的接入点传送对网络接入的请求；在所述第一装置处从所述接入点接收第一密钥；处理与用户装置的支付事务，其中处理支付事务包括向用户装置提供第一密钥以及从用户装置接收第二密钥，并且其中，用户装置是使用第一密钥来获得网络接入的；以及向所述接入点提供所述第二密钥。

[0029] 在一些实施例中，所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥和所述第二密钥产生第三密钥，并且所述用户装置进一步与所述接入点通信，以进一步基于所述第三密钥获得所述网络接入。

[0030] 在一些实施例中，处理支付事务还包括从用户装置接收支付数据。

[0031] 在一些实施例中，所述接入点是在处理所述支付事务之前产生所述第一密钥的。

[0032] 在一些实施例中，所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

[0033] 在一些实施例中，一种计算装置包括：处理器；以及其中存储有程序指令的存储器，所述程序指令可以由所述处理器执行以使得所述计算装置执行以下步骤：向网络的接入点传送对网络接入的请求；从所述接入点接收第一密钥；处理与用户装置的支付事务，其中，处理支付事务包括向用户装置提供第一密钥以及从用户装置接收第二密钥，并且其中，用户装置是使用第一密钥来获得网络接入的；以及向所述接入点提供所述第二密钥。

[0034] 在一些实施例中，所述用户装置与所述接入点通信，以至少部分地基于所述第一密钥和所述第二密钥来产生第三密钥，并且所述用户装置进一步与所述接入点通信，以进一步基于所述第三密钥获得所述网络接入。

[0035] 在一些实施例中，处理支付事务还包括从用户装置接收支付数据。

[0036] 在一些实施例中，所述第一密钥是利用带外(OOB)信道来提供给所述用户装置的。

[0037] 在一些实施例中，所述接入点是在处理所述支付事务之前产生所述第一密钥的。

附图说明

[0038] 通过参考附图，可以更好地理解这些实施例，并且众多目标、特征和优点将对于本领域的技术人员显而易见。

[0039] 图1是用于配置装置进行网络接入的示例性系统的示意图。

[0040] 图2和3示出了用于说明示例性网络接入认证过程的流程图。

[0041] 图4为示出了网络接入认证过程的操作的实施例的示意图。

[0042] 图5为示出了网络接入认证过程的操作的另一实施例的示意图。

[0043] 图6为示出了网络接入认证过程的操作的另一实施例的示意图。

[0044] 图7是包括用于网络通信的接口的电子装置的示例性实施例的方框图。

具体实施方式

[0045] 下面的描述包括体现本公开内容的技术的示例性系统、方法、技术、指令序列和计算机程序产品。不过，要理解的是，可以无需这些具体细节来实践描述的实施例。例如，尽管一些范例提到获得对利用了802.11通信协议的无线局域网(WLAN)的网络接入，但在其他实施例中，可以执行本文描述的网络接入操作以获得对实现了其他适当通信协议(例如，以太网、电力线通信(PLC)、长期演进(LET)、3G、4G等)的其他类型网络的网络接入。在其他实例

中，未示出公知的指令实例、协议、结构和技术的细节，以免使描述模糊不清。

[0046] 可以使用销售点(POS)装置促进接入点(AP)和用户装置(例如，智能电话)之间的网络接入认证过程。可以使用POS装置在AP和用户装置之间交换一个或多个密钥。如下所述，可以在网络接入认证过程期间使用这些密钥以认证用户装置。在认证了用户装置时，可以向认证的用户装置提供网络接入(例如，访客网络接入)。例如，可以经由无线网络(例如，WLAN)或有线网络(例如，以太网或电力线)提供网络接入。

[0047] 在一个实施例中，POS装置能够处理客户和商家之间的事务，例如用于购买商品或服务。在接收到事务指示时，POS装置能够向AP请求网络接入(例如，访客网络接入)。AP能够产生AP密钥对，并为POS装置提供该AP密钥对的公共密钥。POS装置能够通过带外(OOB)信道向用户装置提供接收到的公共密钥。一旦用户装置接收到AP公共密钥，用户装置和AP就能够基于AP密钥对来发起密钥建立过程。可以使用密钥建立过程来产生安全密钥(例如，成对主密钥(PMK))。安全密钥可以用于在网络安全过程期间认证用户装置。通过这种方式，可以在不使用麻烦且不安全的密码，以及在不使用不可靠且不稳定的强制网络门户的情况下，认证用户装置以进行网络接入。

[0048] 在一个实施例中，客户和商家(或服务提供商)之间的事务可以触发用户装置的网络接入认证。在另一实施例中，用户装置可以被配置用于在客户和商家之间进行事务期间进行网络接入。商家通常使用销售点(POS)装置处理事务。客户通常具有用户装置，用户装置可以用于完成和POS装置的事务。此外，实施例不限于访客网络接入。根据应用，可以向用户装置提供另一种类型的网络接入，例如完整网络接入、管理员网络接入、临时网络接入、订约人网络接入等。下面进一步描述以上网络接入认证过程的各个方面。

[0049] 图1是根据一些实施例的用于配置装置进行网络接入的系统100的示意图。在图1中所示的系统100中，用户装置102可以涉及与销售点(POS)装置104的客户事务。用户装置102包括事务单元120、网络通信单元122和认证单元126。POS装置104包括网络通信单元114和事务单元116。接入点(AP)106被配置为向用户装置102提供网络接入(例如，访客网络接入)。AP 106包括认证单元130和网络通信单元132。要指出的是，可以利用软件和/或硬件来实现装置102、104和/或106中的每个的一个或多个单元，例如，如下文参考图7所述。例如，装置(例如，装置104)的处理器可以执行装置的存储器中存储的指令以实现与一个或多个单元(例如，事务单元116)相关联的功能。

[0050] 用户装置102可以采取能够通过通信网络传输数据的任何技术上可行的电子装置的形式。例如，用户装置102可以是可以由用户转移的移动装置，例如智能电话、膝上计算机、上网本、平板计算机、智能手表等。POS装置104可以是专用商务计算机，AP 106可以是专用AP。此外，可以利用诸如智能电话、膝上计算机、上网本、平板计算机、智能家电等电子装置来实现POS装置104和/或AP 106。

[0051] POS装置104经由链路110通信地耦合到AP 106。POS装置104的网络通信单元114能够通过经由链路110与AP 106的网络通信单元132进行通信来促进网络接入认证过程的一部分。例如，POS装置104能够与AP 106通信以请求网络接入并使得AP 106的认证单元130产生密钥。用户装置102能够经由链路112来执行与AP 106的网络接入认证过程的另一部分。例如，用户装置102能够使用认证单元126经由链路112与认证单元130执行密钥建立过程和/或网络安全过程。可以利用无线网络，例如IEEE 802.11、长期演进(LTE)、3G、4G等实现

链路110和112。还可以利用有线联网技术，例如以太网或电力线等实现链路110和112。

[0052] 网络通信单元114、122和132中的每个都可以包括实施ZigBee®、IEEE802.11和/或Bluetooth®协议的无线接口。在一些实施例中，网络通信单元114、122和132还可以包括实施以太网协议和/或电力线通信(PLC)协议(例如，由HomePlug®标准描述的协议)的有线接口。在一些实施例中，网络通信单元114、网络通信单元132和网络通信单元122可以包括一个或多个无线收发机、模拟前端(AFE)单元、天线、处理器、存储器、其他逻辑单元和/或其他部件以实施通信协议和相关功能。

[0053] 用户装置102可以使用事务单元120以经由带外(OOB)信道108与POS装置104的事务单元116通信。例如，如果系统100中的装置实施IEEE802.11协议进行通信，则事务单元120能够利用Bluetooth协议(即，Bluetooth信道)、近场通信(NFC®)协议(即，NFC信道)、红外协议(即，红外信道)等来经由OOB信道108与事务单元116通信。POS装置104的事务单元116还可以使用光信道，例如，通过使用纸质收据或作为POS装置104的显示器上显示的图像，来经由OOB信道108向用户装置102的事务单元120提供信息(例如，密钥)。事务单元116还可以例如通过在POS装置104的显示器上显示QR代码或条形码等，来利用QR代码或条形码在纸质收据上印刷信息。事务单元116还可以利用蜂窝信道，例如，经由电子邮件、短消息服务(SMS)和/或多媒体消息服务(MMS)来经由OOB信道108向事务单元120提供信息。要指出的是，还可以使用不同的信道，例如，使用蓝牙信道，来发送电子邮件。

[0054] POS装置104能够处理客户和商家之间的客户事务。客户事务可以包括客户利用POS装置104从商家购买商品或服务。可以在利用或不利用用户装置102的情况下来执行客户事务。在一些范例中，可以通过利用POS装置104但不利用用户装置102，例如，通过客户向POS装置104人工提供支付，来执行客户事务。在一些范例中，客户事务还可以包括支付事务，例如，其中使用用户装置102经由OOB信道108为商品或服务付款。客户事务可以包括在用户装置102和POS装置104之间传输数据(例如，客户的联系方式和/或支付数据)和/或文件。

[0055] POS装置104能够接收对客户事务的指示。该指示可以由用户装置102(例如，通过事务单元120)产生并被传送给POS装置104(例如，通过OOB信道108)。该指示可以被实现为消息、通知、控制分组等。在一些实施方式中，并非由用户装置102产生，对客户事务的指示可以包括POS装置104从信用卡或智能卡读取器接收的支付数据。例如，接收的支付数据可以包括信用卡或智能卡信息。在另一个范例中，对客户事务的指示可以在处理客户事务时由POS装置104的事务单元116在本地产生。例如，可以在事务单元116处理人工客户事务(例如，从客户接收支付)时，将POS装置104的存储器中预定位置中的标志设置成指示客户事务。

[0056] 除了处理客户事务之外，POS装置104还能够发起网络接入认证过程以向用户装置102提供网络接入(例如，访客网络接入)。在一个实施例中，POS装置104的事务单元116处理客户和商家之间的客户事务，例如用于购买商品或服务。在接收到对客户事务的指示时，网络通信单元114能够为用户装置102向AP 106请求网络接入。网络通信单元114能够经由网络，例如，通过利用链路110向网络通信单元132传送网络接入请求。

[0057] 在接收到网络接入请求之后，AP 106的认证单元130能够产生包括AP公共密钥和

AP私有密钥的AP密钥对。AP 106能够使用通信单元132，例如，通过利用链路110向网络通信单元114提供AP公共密钥。在一种实施方式中，AP密钥对是短暂密钥对，即，每次执行密钥建立过程时都产生新的密钥对。AP 106能够在密钥建立过程期间，例如，如下文参考图4所述，使用AP私有密钥。

[0058] 事务单元116能够通过OOB信道108向事务单元120提供AP公共密钥。例如，事务单元116能够在收据上(例如，通过利用QR代码)印刷AP公共密钥，通过发送电子邮件或短信(即，使用SMS或MMS)的方式向事务单元120提供AP公共密钥。一旦用户装置102接收到AP公共密钥，认证单元126和认证单元130就发起密钥建立过程，如下文更详细所述。

[0059] 继续以上的范例，认证单元126能够产生包括装置私有密钥和装置公共密钥的装置密钥对。用户装置102能够在密钥建立过程期间，例如，如下文参考图4所述，使用装置私有密钥。密钥建立过程可以包括执行关联请求，该关联请求包括认证单元126经由链路112向认证单元130提供装置公共密钥。密钥建立过程包括认证单元126和认证单元130产生安全密钥，例如，成对的主密钥(PMK)。

[0060] 认证单元126和认证单元130然后基于密钥建立过程发起网络安全过程。认证单元126和认证单元130能够使用安全密钥来执行网络安全过程，例如WPA2认证。一旦完成了网络安全过程，就可以由AP 106经由链路112，或经由另一链路和/或另一AP向用户装置102提供网络接入。

[0061] 在网络接入认证过程的另一实施例中，如下文参考图6所述，在用户装置102和POS装置104之间的客户事务期间执行公共密钥交换。可以在事务单元120和事务单元116之间通过OOB信道108进行客户事务(例如，支付事务)。例如，支付事务可以包括客户使用用户装置102使用通信协议，例如NFC协议或Bluetooth协议，经由OOB信道108向POS 108提供支付。在发起客户事务之前，认证单元130能够产生AP密钥对，然后向POS装置104提供AP密钥对中的AP公共密钥。此外，在发起客户事务之前，认证单元126还可以产生包括装置公共密钥和装置私有密钥的装置密钥对。

[0062] 作为客户事务的一部分，事务单元116从事务单元120接收装置公共密钥，事务单元120从事务单元116接收AP公共密钥。网络通信单元114能够向网络通信单元132传送装置公共密钥。一旦用户装置102接收到AP公共密钥，并且AP 106接收到装置公共密钥，认证单元126和认证单元130就发起密钥建立过程。类似于上述实施例，密钥建立过程可以包括产生安全密钥(例如，PMK)。认证单元126和认证单元130能够使用安全密钥来执行网络安全过程。一旦完成了网络安全过程，就可以由AP 106为用户装置102提供网络接入。

[0063] 在网络接入认证过程的另一实施例中，利用了对安全密钥(例如PMK)的直接交换，如下文参考图5所述。POS装置104的事务单元116处理客户和商家之间的客户事务。在接收到对客户事务的指示时，POS装置104向AP 106请求(例如，使用链路110)网络接入。在接收到网络接入请求时，认证单元130产生安全密钥。认证单元130通过链路110向网络通信单元114提供安全密钥。事务单元116然后经由OOB信道108向事务单元120提供安全密钥。例如，事务单元116能够在收据上(例如，利用QR代码)印刷安全密钥，通过发送电子邮件或短信(即，使用SMS或MMS)的方式向事务单元120提供安全密钥。认证单元126和认证单元130然后能够使用安全密钥，即，经由链路112发起网络安全过程。参考以下附图更详细地描述本实施例和其他实施例的示例性操作。

[0064] 图2描绘了示出了根据一些实施例的网络接入认证过程的流程图200。参考图1中描述的系统和部件来描述流程图200(出于解释的目的而非作为限制)。可以由系统100中的一个或多个部件,例如POS装置104的网络通信单元114和事务单元116,来执行示例性操作。

[0065] 从方框202开始,POS装置104接收对使用POS装置104的客户事务的指示。如上文参考图1所述,可以将指示实现为消息、通知或控制分组。该指示可以包括与客户事务相关联的数据。

[0066] 还如上文参考图1所述,客户事务可以是用于购买商品或服务的事务。在一种实施方式中,客户能够在不使用用户装置102的情况下人工向POS装置104提供支付。例如,客户能够利用信用卡或智能卡向POS装置104提供支付数据。在一个范例中,从信用卡或智能卡接收的支付数据可以是对客户事务的指示。在另一个范例中,POS装置104能够在处理接收到的支付数据时产生对客户事务的指示。

[0067] 在另一实施方式中,客户可以利用用户装置102,例如,通过选择用户装置102的显示器中的选项以发起与POS装置104的电子支付事务来为购买的商品进行支付。事务单元116能够通过OOB信道108或经由另一信道从用户装置102的事务单元120接收对客户事务的指示。例如,事务单元116可以从事务单元120接收支付数据。

[0068] 进行到方框204,响应于接收到对客户事务的指示,POS装置104向AP 106传送对网络接入的请求。例如,POS装置104的网络通信单元114能够经由链路110向AP 106的网络通信单元132传送对网络接入的请求。

[0069] 在一个实施例中,如下文参考图4所述,AP 106能够在接收到对网络接入的请求时产生AP密钥对。在另一实施例中,如下文参考图5所述,AP 106能够在接收到对网络接入的请求时产生安全密钥。

[0070] 进行到方框206,POS装置104从AP 106接收密钥。例如,网络通信单元114经由链路110从网络通信单元132接收密钥。在图4的实施例中,POS装置104接收AP密钥对中的AP公共秘钥。在图5的实施例中,POS装置104接收安全密钥。

[0071] 进行到方框208,POS装置104向用户装置102提供密钥。用户装置102被配置为使用该密钥获得对网络的网络接入。可以在不改变密钥的格式的情况下向用户装置102提供密钥。POS装置104从而在向用户装置102提供密钥时保持了所接收密钥(由AP 106产生)的一致性。

[0072] 在图4的实施例中,POS装置104能够向用户装置102提供AP公共密钥。例如,事务单元116能够通过OOB信道108向事务单元120提供AP公共密钥。一旦用户装置102接收到AP公共密钥,认证单元126和认证单元130就基于AP密钥对(即,由AP 106产生的密钥对)发起密钥建立过程以及随后的网络安全过程。

[0073] 在图5的实施例中,POS装置104可以向用户装置102提供安全密钥。例如,事务单元116能够经由OOB信道108向事务单元120提供安全密钥。认证单元126和认证单元130能够使用安全密钥,例如,经由链路112发起网络安全过程。

[0074] 图3描绘了示出了根据一些实施例的网络接入认证过程的流程图300。参考图1中描述的系统和部件来描述流程图300(出于解释的目的而非作为限制)。可以由系统100中的一个或多个部件,例如POS装置104的网络通信单元114和事务单元116,来执行示例性操作。

[0075] 从方框302开始,POS装置104向AP 106传送对网络接入的请求。例如,网络通信单

元114能够经由链路110向AP 106的网络通信单元132传送对网络接入的请求。在一个实施例中，如下文参考图6所述，AP 106能够在接收到对网络接入的请求时产生AP密钥对。

[0076] 进行到方框304，POS装置104从AP 106接收AP密钥对中的AP公共密钥。例如，网络通信单元114能够经由链路110从网络通信单元132接收AP公共密钥。

[0077] 进行到方框306，POS装置104处理与用户装置102的支付事务。例如，用户装置102可以包括可用于从POS装置104为商品付款的支付应用。客户可以选择支付应用中的电子支付，例如，选择一种形式的支付。用户装置102上的支付应用然后能够发起支付事务。例如，可以通过利用NFC协议或Bluetooth协议等，来经由OOB 108在事务单元120和事务单元116之间执行支付事务。

[0078] 支付事务的处理包括POS装置104向用户装置102提供AP公共密钥，并从用户装置102接收装置密钥对中的装置公共密钥。例如，事务单元116能够经由OOB信道108从事务单元120接收装置公共密钥，连同支付事务的支付数据。作为支付事务的一部分，事务单元116能够经由OOB信道108向事务单元120传送AP公共密钥。

[0079] 要指出的是，POS装置104能够在处理来自用户装置102的支付事务(方框306)之前，传送对网络接入的请求(方框302)并从AP 106接收AP公共密钥。不过，在一个实施例中，POS装置104能够与处理来自用户装置102的支付事务(方框306)基本上同时地从AP 106接收AP公共密钥(方框304)。

[0080] 进行到方框308，POS装置104能够向AP 106提供装置公共密钥。例如，网络通信单元114能够向网络通信单元132提供装置公共密钥。如下文参考图6更详细所述，一旦用户装置102接收到AP公共密钥，认证单元126和认证单元130就基于AP密钥对和装置密钥对，发起密钥建立过程和网络安全过程。

[0081] 图4为示出了根据一些实施例的，在网络接入认证过程期间由用户装置102、POS装置104和AP 106执行的操作的消息流图。

[0082] POS装置104经由402A或402B(如虚线所示)接收对使用POS装置104的客户事务的指示。在402A，POS装置104能够从用户装置102接收对客户事务的指示。可以通过带外(OOB)信道，例如OOB 108传输对客户事务(例如，支付数据)的指示。

[0083] 或者，在402B，POS装置104能够接收作为在没有使用用户装置102的情况下所提供的支付数据的一部分的对客户事务的指示。例如，客户能够在不使用用户装置102的情况下人工地向POS装置104提供支付。对客户事务的指示可以是接收的支付数据，例如信用卡或智能卡信息。POS装置104还可以在接收或处理支付数据时在本地产生并存储对客户事务的指示(例如，标志)。

[0084] 在404，在接收到对客户事务的指示时，POS装置104向AP 106传送网络接入请求。网络通信单元114能够经由网络，例如通过使用链路110向网络通信单元132传送网络接入请求。

[0085] 在406，在接收到网络接入请求时，AP 106产生AP密钥对。AP密钥对可以包括AP私有密钥和AP公共密钥。在一个实施例中，AP密钥对是非对称密钥对。

[0086] 在408，AP 106向POS装置104传送AP密钥对中的公共密钥。网络通信单元132能够经由网络，例如通过使用链路110向网络通信单元114传送公共密钥。

[0087] 在410，POS装置102向用户装置102传送AP密钥对中的公共密钥。POS装置104能够

经由OOB信道向用户装置102传送公共密钥。在一个实施例中，410的OOB信道可以与402中使用的OOB信道相同。在另一实施例中，410中使用的OOB信道与402中使用的OOB信道不同。

[0088] 在412，用户装置102和AP 106发起密钥建立过程。412的密钥建立过程可以包括用户装置102向AP 106传送关联请求。412的密钥建立过程还可以包括用户装置102向AP 106传送装置密钥对中的装置公共密钥。在一些实施方式中，用户装置102能够在发起412的密钥建立过程之前或在412的密钥建立过程期间产生装置密钥对，其包括装置公共密钥和装置私有密钥。例如，用户装置102能够在402处传送客户事务时、在410处接收AP公共密钥时、或在412处执行关联请求等时，来产生装置密钥对。

[0089] 在414A，用户装置102至少部分地基于接收到的AP公共密钥产生安全密钥。类似地，在414B，AP 106至少部分地基于接收到的装置公共密钥产生安全密钥。在一个实施例中，由用户装置102和AP 106产生的安全密钥是对称密钥。在一个实施例中，用户装置102和AP 106至少部分地基于412的关联请求来同时地产生对称密钥。在一个实施例中，在414A和414B，用户装置102和AP 106产生单个安全密钥，然后该单个安全密钥被用户装置102和AP 106两者存储。

[0090] 用户装置102和AP 106能够至少部分地基于Diffie-Hellman(DH)、对等实体同时认证(SAE)、Wi-Fi保护设置(WPS)或任何其他技术上可行的用户装置102和AP 106之间的密钥建立过程，来产生安全密钥。安全密钥接下来可以被直接使用，或利用密钥推导算法来被导出，以便用于网络安全过程中。可以利用依赖于对称密钥的认证协议，例如由Wi-Fi保护的接入((WPATM或WPA2TM)或由有线等同私密性(WEP)指定的4次握手认证，来实现网络安全过程。可以将安全密钥实现为成对主密钥(PMK)、成对临时密钥(PTK)或预先共享密钥(PSK)。

[0091] 在416，用户装置102和AP 106执行网络安全过程。网络安全过程是利用安全密钥、或其衍生物，例如PMK密钥来执行的。例如，用户装置102和AP 106能够利用安全密钥，根据WPA或WPA2协议、WEP协议或其他网络安全过程，来执行网络安全过程。要指出的是，尽管一般将WEP和WPA/WPA2用于WLAN网络，但使用其他网络和/或网络安全过程也是可预期的。

[0092] 在418A，用户装置102利用安全密钥来认证AP 106以进行网络接入。例如，认证单元126基于416的网络安全过程来认证AP 106。在418B，AP106利用安全密钥来认证用户装置102以进行网络接入。例如，认证单元130基于416的网络安全过程来认证用户装置102。在根据418A和418B的相互认证过程获得网络接入之后，用户能够经由用户装置102上运行的浏览器或其他应用来访问因特网或其他网络资源。

[0093] 要指出的是，在一些实施例中，传送的是公共密钥的散列而非公共密钥自身。使用散列可以提供额外的密码安全层。例如，在408，AP 106能够向POS装置104传送AP密钥对中的AP公共密钥的散列。在410，POS装置104能够向用户装置102传送AP公共密钥的散列。然后，用户装置102能够验证在密钥建立过程412之内接收的AP公共密钥匹配接收的散列，并继续进行412。

[0094] 图5是示出了根据一些实施例的，由用户装置102、POS装置104和AP 106执行的操作的消息流图。

[0095] POS装置104经由502A或502B(如虚线所示)接收对使用POS装置104的客户事务的指示。在502A，POS装置104能够从用户装置102接收对客户事务的指示。可以通过OOB信道来

传送对客户事务(例如,支付数据)的指示。

[0096] 或者,在502B,POS装置104能够接收作为在没有使用用户装置102的情况下所提供的支付数据的一部分的对客户事务的指示。例如,类似于上文参考402B所述的技术,POS装置104能够经由信用卡或智能卡从客户接收支付。对客户事务的指示可以是接收的支付数据,例如信用卡或智能卡信息。POS装置104还可以在接收或处理支付数据时在本地产生并存储对客户事务的指示(例如,标志)。

[0097] 在504,在接收到对客户事务的指示时,POS装置104向AP 106传送网络接入请求。网络通信单元114能够经由网络,例如通过使用链路110向网络通信单元132传送网络接入请求。

[0098] 在506,在接收到网络接入请求时,AP 106产生安全密钥。要指出的是,与参考图4和6所述的实施例相反,仅有AP 106产生安全密钥,即,不使用密钥建立过程和/或不实现基于用户装置102和AP 106之间交换的非对称密钥的认证协议。在一个实施例中,安全密钥为对称密钥。可以将安全密钥实现为成对主密钥(PMK)、成对临时密钥(PTK)或预先共享密钥(PSK)。

[0099] 在508,AP 106向POS装置104传送安全密钥。网络通信单元132能够通过使用链路110向网络通信单元114传送安全密钥。

[0100] 在510,POS装置104向用户装置102传送安全密钥。POS装置104能够经由OOB信道向用户装置102传送安全密钥。在一个实施例中,410的OOB信道可以与502中使用的OOB信道相同。在另一实施例中,510的OOB信道与502中使用的OOB信道不同。

[0101] 在512,用户装置102和AP 106执行网络安全过程。网络安全过程是利用安全密钥、或使用密钥推导算法获得的安全密钥的衍生物来执行的。例如,用户装置102和AP 106能够利用安全密钥,根据Wi-Fi保护接入(WPA)或WPA2协议、有线等同私密性(WEP)协议或其他网络安全过程,来执行网络安全过程。要指出的是,尽管一般将WEP和WPA/WPA2用于WLAN网络,但使用其他网络和相对应的网络安全过程也是可预期的。

[0102] 在514A,用户装置102利用安全密钥来认证AP 106进行网络接入。例如,认证单元126基于512的网络安全过程来认证AP 106。在514B,AP106利用安全密钥来认证用户装置102进行网络接入。例如,认证单元130基于512的网络安全过程来认证用户装置102。

[0103] 图6是示出了根据一些实施例的,由用户装置102、POS装置104和AP 106执行的操作的消息流图。

[0104] 在602,POS装置104向AP 106传送网络接入请求。网络通信单元114能够通过利用链路110向网络通信单元132传送网络接入请求。

[0105] 在604,在接收到网络接入请求时,AP 106产生AP密钥对。AP密钥对可以包括AP私有密钥和AP公共密钥。在一个实施例中,AP密钥对是非对称密钥对。

[0106] 在606,AP 106向POS装置104传送AP密钥对中的公共密钥。网络通信单元132能够通过使用链路110向网络通信单元114传送公共密钥。

[0107] 在608,用户装置102和POS装置104执行支付事务。支付事务608包括用户装置102在612向POS装置104传送支付数据。支付数据能够指示从客户的银行向商家银行传输的金钱,并且该支付数据可以包括针对认证该支付事务的其他信息。用户装置102能够通过OOB信道108,例如通过利用NFC协议或Bluetooth协议等来传送支付数据。例如,用户装置102可

以包括可用于向POS装置104提供支付的支付应用。该支付应用能够与金融机构(例如,客户的银行)通信以向POS装置104授权支付。然后,该支付应用能够向POS装置104提供支付授权。

[0108] 608的支付事务还包括用户装置102在614向POS装置104传送装置密钥对中的装置公共密钥。用户装置102能够在608处执行支付事务之前产生装置密钥对。用户装置102能够保持装置密钥对中的装置私有密钥,即,不向其他装置传送装置私有密钥。支付事务608还包括POS装置104向用户装置102传送AP密钥对中的AP公共密钥。

[0109] 在一个实施例中,在614,用户装置102能够通过用户装置102用于传送支付数据612的相同OOB信道来向POS装置104传送装置公共密钥。在一个实施例中,在616,POS装置104能够通过与在612处传送支付数据和/或在614处传送装置公共密钥相同的OOB信道,例如,通过利用NFC协议或Bluetooth协议等,来向用户装置102传送AP公共密钥。

[0110] 在618,POS装置104向AP 106传送装置公共密钥。例如,网络通信单元114经由链路110向网络通信单元132传送装置公共密钥。

[0111] 在620,用户装置102和AP 106发起密钥建立过程。620的密钥建立过程可以包括用户装置102向AP 106传送关联请求。

[0112] 在622A,用户装置102至少部分地基于接收的AP公共密钥产生安全密钥。类似地,在622B,AP 106至少部分地基于接收到的装置公共密钥产生安全密钥。在一个实施例中,由用户装置102和由AP 106产生的安全密钥是对称密钥。在一个实施例中,用户装置102和AP 106至少部分地基于620的密钥建立过程的关联请求来同时地产生对称密钥。在一个实施例中,在414A和414B,用户装置102和AP 106产生单个安全密钥,然后该单个安全密钥被用户装置102和AP 106两者存储。

[0113] 类似于上文参考图4的414A和414B所述的技术,分别在622A和622B处,用户装置102和AP 106能够至少部分地基于Diffie-Hellman(DH)、对等实体同时认证(SAE)、Wi-Fi保护设置(WPS)或任何其他技术上可行的密钥建立过程,来产生安全密钥。可以将安全密钥实现为成对主密钥(PMK)、成对临时密钥(PTK)或预先共享密钥(PSK)。

[0114] 类似于上文参考图4的416所述的技术,在624,用户装置102和AP 106能够执行网络安全过程。网络安全过程是利用安全密钥,例如PMK密钥来执行的。例如,用户装置102和AP 106能够利用安全密钥,根据Wi-Fi保护接入(WPA)或WPA2协议、有线等同私密性(WEP)协议或其他网络安全过程,来执行网络安全过程。要指出的是,尽管一般将WEP和WPA/WPA2用于WLAN网络,但使用其他网络和相对应的网络安全过程也是可预期的。

[0115] 在626A,用户装置102利用安全密钥来认证AP 106进行网络接入。例如,认证单元126基于624的网络安全过程来认证AP 106。在626B,AP106利用安全密钥来认证用户装置102进行网络接入。例如,认证单元130基于624的网络安全过程来认证用户装置102。

[0116] 类似于上文参考图4描述的技术,可以传送公共密钥的散列而非公共密钥自身。例如,在608,AP 106能够向POS装置104传送AP密钥对中的AP公共密钥的散列。类似地,在618,POS装置104能够向AP 106传送装置密钥对中的装置公共密钥的散列。

[0117] 根据本公开内容将认识到,可以修改图2和3和/或图4-6的流程图以便导出本公开内容的替代方面。而且,按照相继的次序示出本公开内容的该方面中的一些操作。不过,某些操作可以按照与图示不同的次序发生,某些操作可以同时被执行,某些操作可以与其他

操作组合，以及可以在本公开内容的另一方面中缺少某些操作。

[0118] 本领域的技术人员将会认识到，可以将本公开内容的方面实现为系统、方法或计算机程序产品。因此，本公开内容的方面可以采取完全硬件实施例、软件实施例(包括固件、常驻软件、微代码等)或组合软件和硬件方面的实施例的形式，在本文中可以将所有这些一般性地称为“电路”、“模块”、“单元”或“系统”。此外，本公开内容的方面可以采取其上包含有计算机可读程序代码的一个或多个计算机可读介质中包含的计算机程序产品的形式。

[0119] 可以利用一个或多个非暂态计算机可读介质的任何组合。非暂态计算机可读介质包括所有计算机可读介质，唯一的例外是暂态传播信号。非暂态计算机可读介质可以是计算机可读存储介质。计算机可读存储介质可以是，例如，但不限于，电、磁、光、电磁、红外或半导体系统、装置或设备或者上述任何适当的组合。计算机可读存储介质的更具体范例(非穷举列表)包括以下：具有一条或多条线的电连接、便携式计算机软盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪速存储器)、光纤、便携式压缩盘只读存储器(CD-ROM)、光存储装置、磁存储装置或以上各项的任何适当组合。在本文的语境中，计算机可读存储介质可以是能够包含或存储程序供或结合指令执行系统、设备或装置使用的任何有形介质。

[0120] 可以用一种或多种程序设计语言的任意组合编写计算机可读介质上包含的用于执行本公开内容的方面的操作的计算机程序代码，包括面向对象的编程语言，例如Java、Smalltalk、C++等，以及常规的过程编程语言，例如“C”编程语言或类似编程语言。可以完全在用户的计算机上、部分地在用户的计算机上、作为独立软件包，部分地在用户的计算机且部分地在远程计算机上、或完全在远程计算机或服务器上执行程序代码。在后一种情形中，远程计算机可以通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接到用户的计算机，或者可以形成通往外部计算机(例如，通过因特网使用因特网服务提供商)的连接。

[0121] 参考根据本公开内容的实施例的方法、装置(系统)和计算机程序产品的流程图和/或方框图描述了本公开内容的方面。将要理解，可以通过计算机程序指令来实现流程图和/或方框图的每个方框以及流程图和/或方框图的方框组合。这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理设备的处理器，以生产机器，使得指令在经由计算机或其他可编程数据处理设备的处理器执行时，生成用于实现流程图和/或方框图方框中指定的功能/动作的手段。

[0122] 这些计算机程序指令也可以存储于计算机可读介质中，其能够指示计算机、其他可编程数据处理设备或其他装置以特定方式工作，使得计算机可读介质中存储的指令生产出一种制品，其包括用于实现流程图和/或方框图方框中指定的功能/动作的指令。

[0123] 计算机程序指令也可以被加载到计算机、其他可编程数据处理设备或其他装置上，以使得在计算机、其他可编程设备或其他装置上执行一系列操作步骤，以产生计算机实现的过程，使得在计算机或其他可编程设备上执行的指令提供用于实现流程图和/或方框图方框中指定的功能/动作的过程。

[0124] 图7是电子装置700的一个实施例的方框图。电子装置700能够实现功能并执行用户装置、POS装置或AP的在以上图1-6中所述的操作，如下文将要进一步所述。该电子装置包括处理器702(其可能包括多个处理器、多个内核、多个节点和/或实现多线程等)。电子装置包括存储器706。存储器706可以是系统存储器(例如，高速缓冲存储器、SRAM、DRAM、零电容

器RAM、双晶体管RAM、eDRAM、EDO RAM、DDR RAM、EEPROM、NRAM、RRAM、SONOS、PRAM等中的一者或多者)或上文已经描述的机器可读介质的可能实现中的任一者或多者。该电子装置还包括总线710(例如,PCI、ISA、PCI-Express、HyperTransport®、InfiniBand®、NuBus等)以及包括无线网络接口(例如,WLAN接口、Bluetooth®接口、WiMAX接口、ZigBee®接口、无线USB接口等)和有线网络接口(例如,PLC接口、以太网接口等)中的至少一者的网络接口704。

[0125] 在一些实施例中,网络接口704可以包括网络通信单元714。此外,网络接口704可以可选地包括事务单元716和认证单元718(如虚线所示)。例如,如果电子装置700是用户装置(例如,图1的用户装置102),则网络接口704可以包括网络通信单元714、事务单元716和认证单元718。在另一个范例中,如果电子装置700是POS装置(例如,图1的POS装置104),则网络接口704可以包括网络通信单元714和事务单元716。在另一个范例中,如果电子装置700是AP(例如,图1的AP 106),则网络接口704可以包括网络通信单元714和认证单元718。在一些实施例中,网络接口704、处理器702和存储器706可以实现上面在图1-6中所描述的功能。例如,网络接口704、处理器702和存储器706可以实现网络通信单元714、事务单元716和/或认证单元718的功能。

[0126] 还要指出,这些功能中的任一者可以部分地(或完全地)用硬件来实现和/或在处理器单元702上实现。例如,可以利用专用集成电路、在处理器单元702中实现的逻辑单元、在外围装置或卡上的协处理器等,来实现该功能。此外,实现可以包括更少的部件或图7中未示出的额外的部件(例如,视频卡、音频卡、额外网络接口、外围装置等)。处理器单元702、存储装置和网络接口704耦合到总线710。尽管被示为耦合到总线710,但存储器单元706可以耦合到处理器单元702。

[0127] 尽管参考各种实施方式和利用描述了各实施例,但将要理解,这些实施例是例示性的且本公开内容的范围不限于它们。通常,本文描述的用于促进配置装置进行网络接入(例如,用于访客网络接入)的技术都可以利用与任何硬件系统相一致的设施来实现。很多变化、修改、添加和改善都是可能的。

[0128] 可以为本文描述为单个实例的部件、操作或结构提供多种实例。最后,各种部件、操作和数据存储器之间的边界有些任意,在特定例示性配置的语境中说明了特定操作。功能的其他分配被想到并可以落入本公开内容的范围之内。通常,作为示例性配置中的分立部件给出的结构和功能可以被实现为组合的结构或部件。类似地,作为单个部件给出的结构和功能可以被实现为分立的部件。这些和其他变化、修改、添加和改善可以落入本公开内容的范围之内。

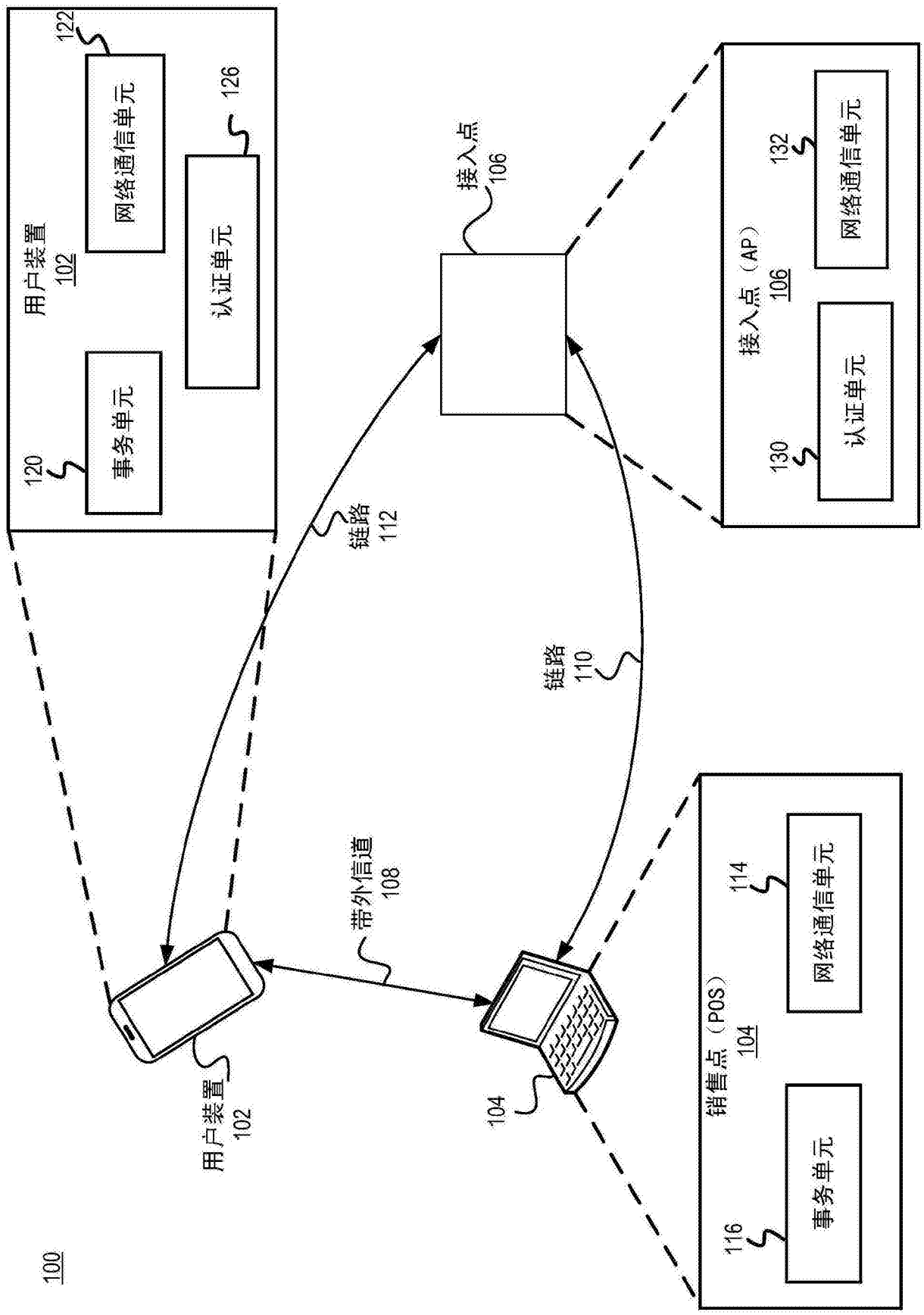

100
用户装置
102
网络通信单元
122
认证单元
126
事务单元
120
接入点
106
链路
112
链路
110
带外信道
108
用户装置
102
104
销售点（POS）
104
网络通信单元
114
事务单元
116
接入点（AP）
106
网络通信单元
132
认证单元
130

图1

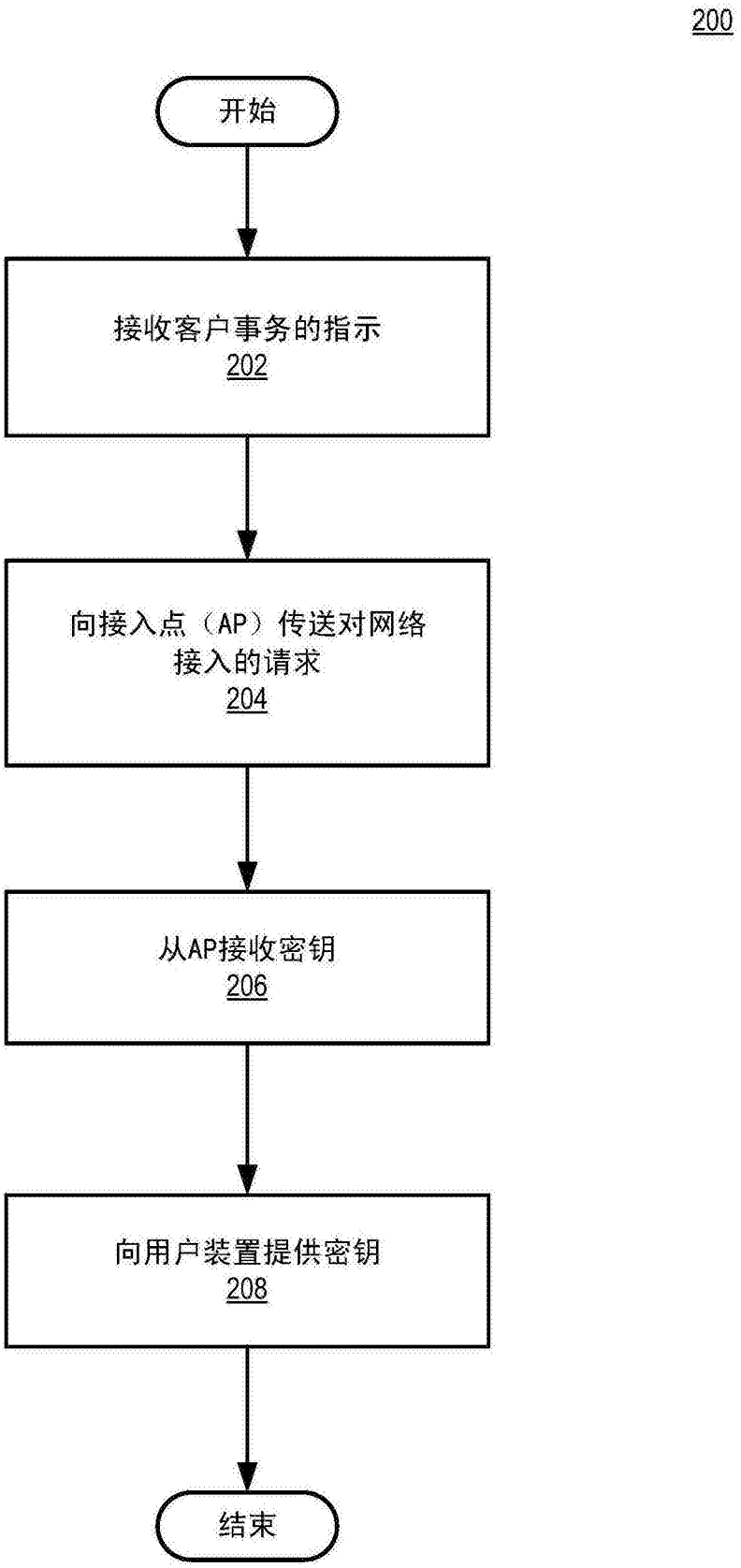

200
开始
接收客户事务的指示
202
向接入点（AP）传送对网络接入的请求
204
从AP接收密钥
206
向用户装置提供密钥
208
结束

图2

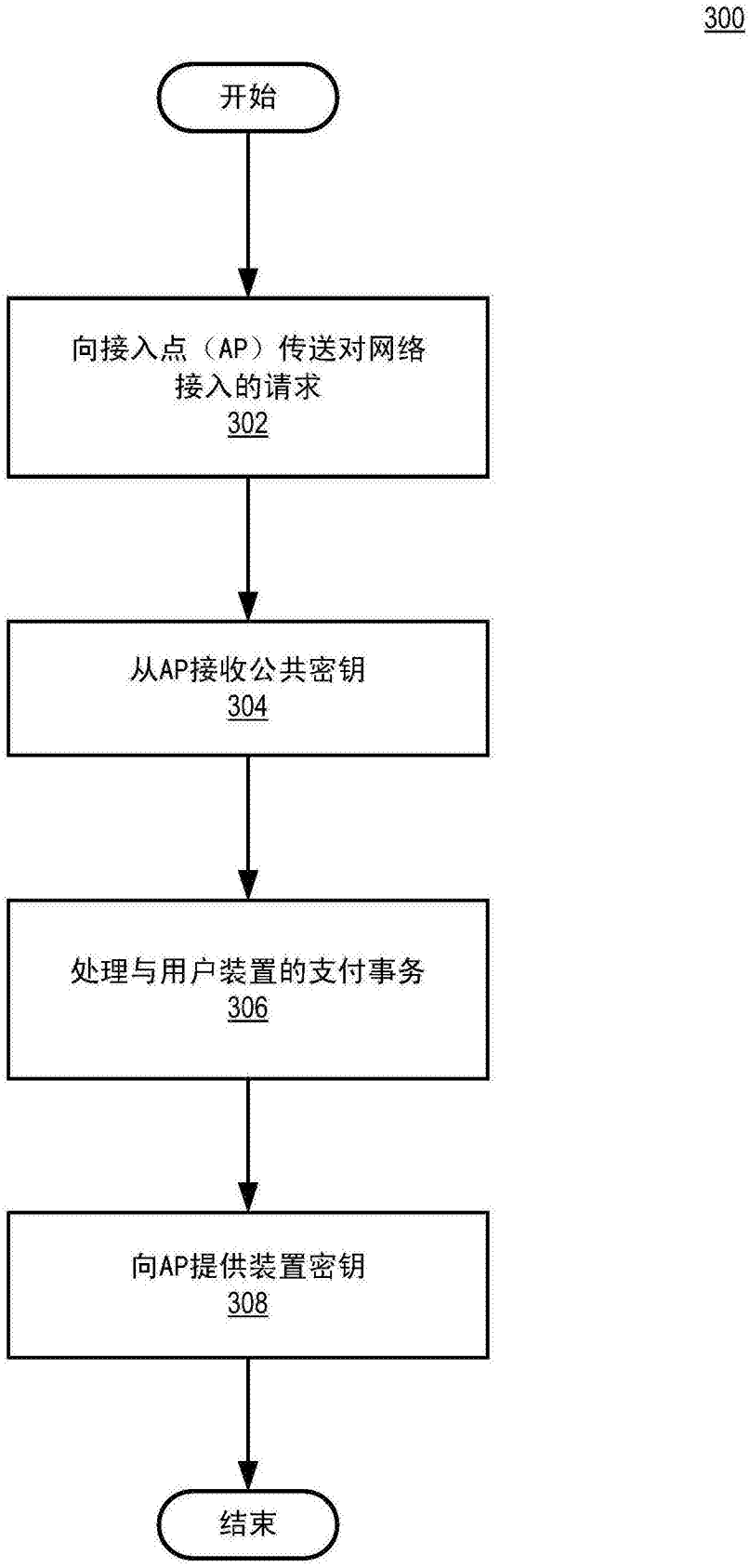

300
开始
向接入点（AP）传送对网络接入的请求
302
从AP接收公共密钥
304
处理与用户装置的支付事务
306
向AP提供装置密钥
308
结束

图3

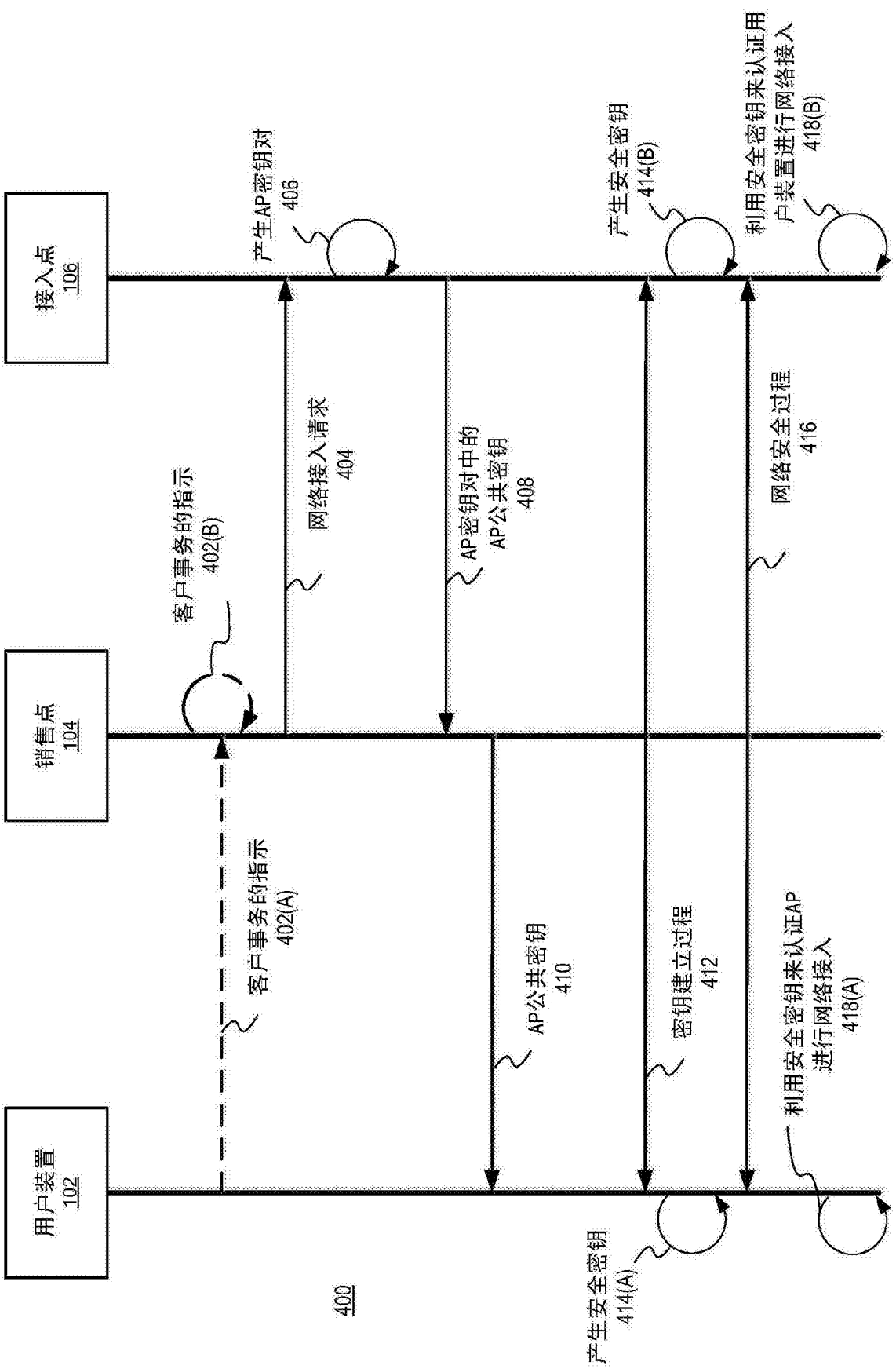

接入点
106
销售点
104
用户装置
102
产生AP密钥对
406
网络接入请求
404
客户事务的指示
402(B)
AP密钥对中的
AP公共密钥
408
产生安全密钥
414(B)
网络安全过程
416
利用安全密钥来认证用
户装置进行网络接入
418(B)
客户事务的指示
402(A)
AP公共密钥
410
密钥建立过程
412
利用安全密钥来认证AP
进行网络接入
418(A)
产生安全密钥
414(A)
400

图4

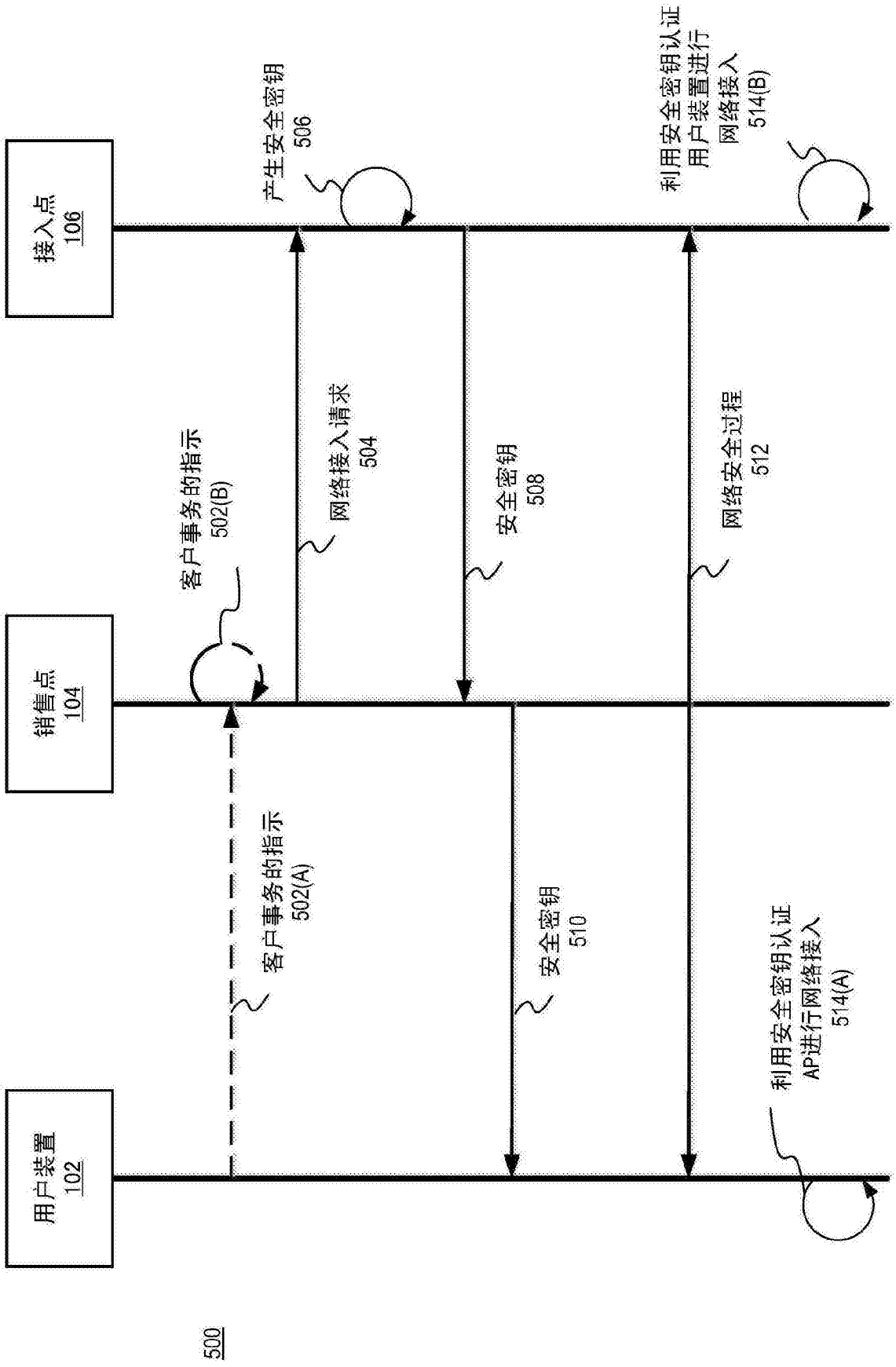

接入点
106
销售点
104
用户装置
102
产生安全密钥
506
利用安全密钥认证
用户装置进行
网络接入
514(B)
客户事务的指示
502(B)
网络接入请求
504
安全密钥
508
网络安全过程
512
客户事务的指示
502(A)
安全密钥
510
利用安全密钥认证
AP进行网络接入
514(A)
500

图5

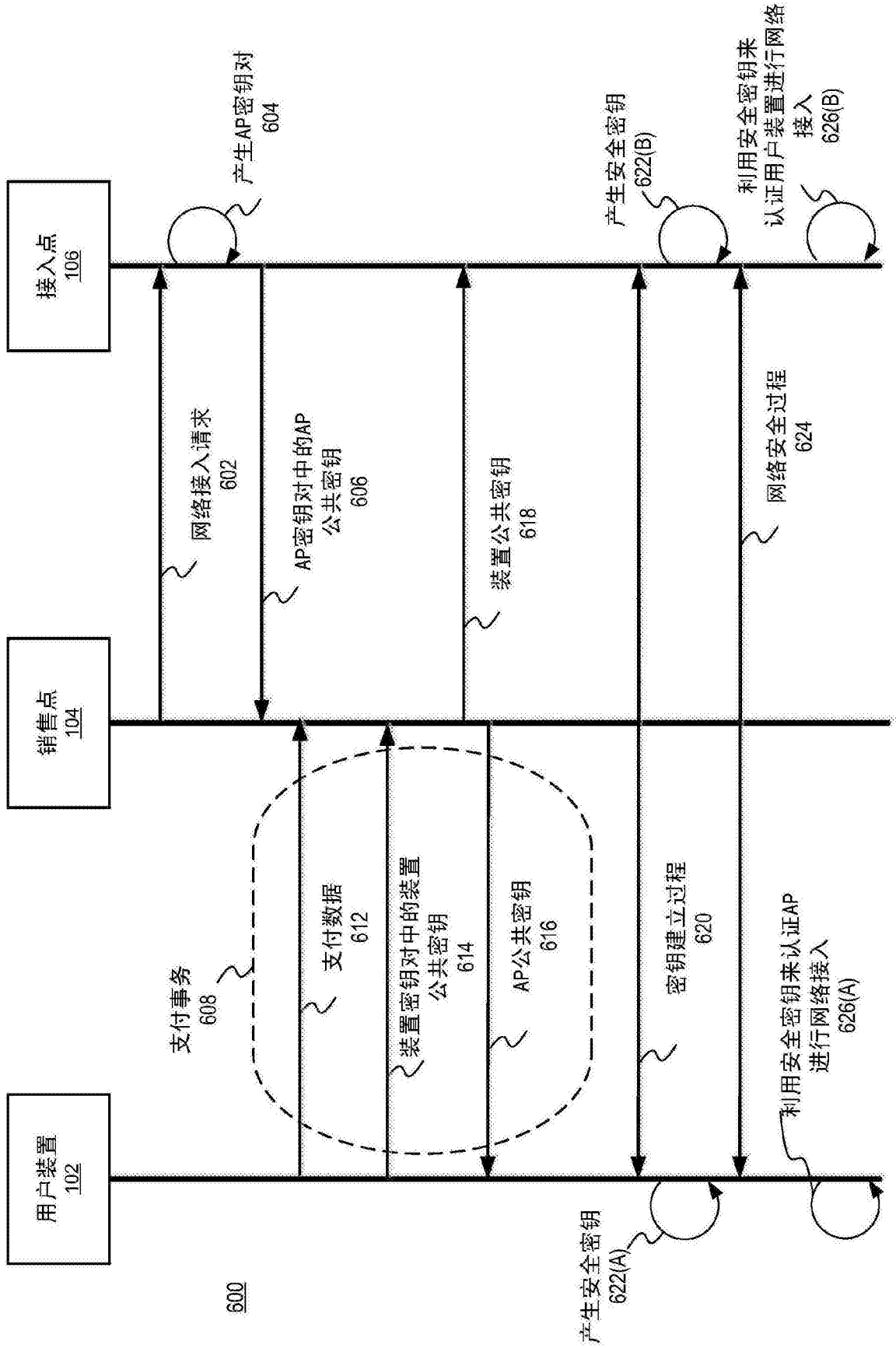

接入点
106
销售点
104
用户装置
102
600
产生AP密钥对
604
网络接入请求
602
AP密钥对中的AP
公共密钥
606
装置公共密钥
618
产生安全密钥
622(B)
利用安全密钥来
认证用户装置进行网络
接入
626(B)
网络安全过程
624
支付事务
608
支付数据
612
装置密钥对中的装置
公共密钥
614
AP公共密钥
616
密钥建立过程
620
利用安全密钥来认证AP
进行网络接入
626(A)
产生安全密钥
622(A)

图6

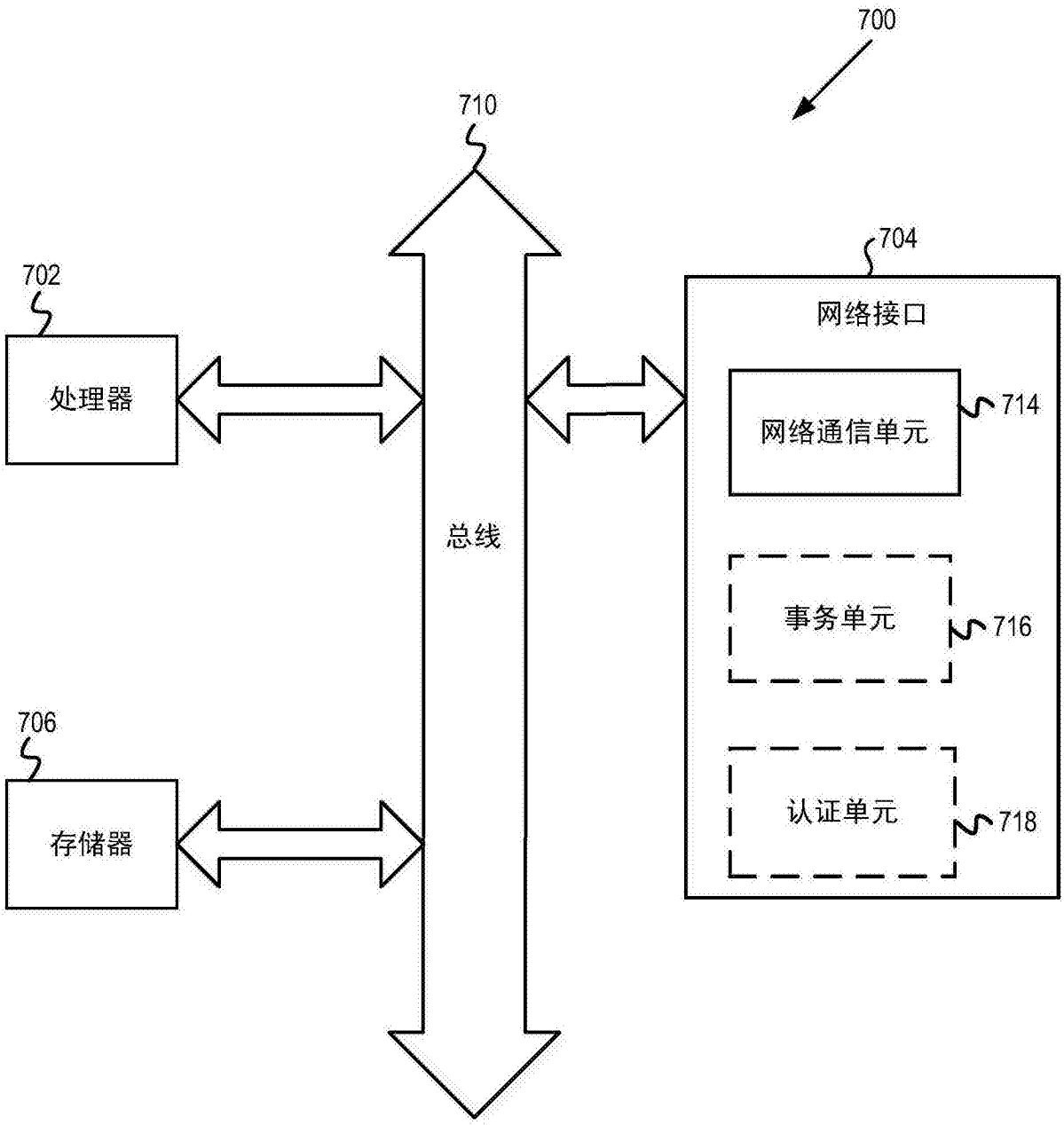

700
710
704
702
网络接口
处理器
网络通信单元
714
总线
事务单元
716
706
存储器
认证单元
718

图7