(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 106576043 A
(43)申请公布日 2017.04.19

(21)申请号 201580041595.8

(22)申请日 2015.06.08

(30)优先权数据
14/473,308 2014.08.29 US

(85)PCT国际申请进入国家阶段日
2017.01.26

(86)PCT国际申请的申请数据
PCT/US2015/034689 2015.06.08

(87)PCT国际申请的公布数据
WO2016/032591 EN 2016.03.03

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 N·M·史密斯 W·C·德里武 T·G·威利斯 N·J·高斯

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 黄嵩泉

(51)Int.Cl.
H04L 9/14(2006.01)
H04L 9/32(2006.01)
H04L 12/58(2006.01)

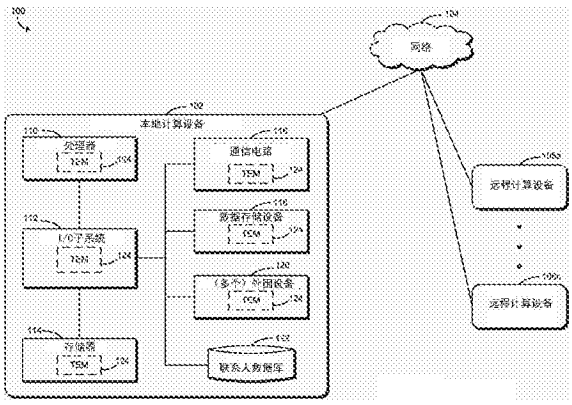
权利要求书4页 说明书20页 附图8页

(54)发明名称

病毒式可分配可信消息传送

(57)摘要

用于利用可信消息传送的技术包括本地计算设备，所述本地计算设备包括建立在可信执行环境中的消息客户端和本地可信消息模块。所述本地可信消息模块基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明。所述本地可信消息模块响应于成功证明所述远程计算设备而进一步与所述远程可信消息模块交换密钥。所述消息客户端将传出消息转发至所述本地可信消息模块，并且接收来自所述本地可信消息模块的传入消息。为了将传出消息安全地传输至所述远程计算设备，所述本地可信消息模块接收来自所述消息客户端的所述传出消息，加密所述传出消息，并且在传输至所述远程计算设备的所述远程可信消息模块之前对所述传出消息进行密码签名。为了安全地接收来自所述远程计算设备的传入消息，所述本地可信消息模块接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息，解密所述传入消息，并且基于所述交换的密钥并在将所述传入消息传输至所述消息客户端之前验证所述传入消息的密码签名。



CN 106576043 A

1.一种用于可信消息传送的本地计算设备,所述本地计算设备包括:

本地可信消息模块,所述本地可信消息模块建立在可信执行环境中,用于:(i)基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明,以及(ii)响应于成功证明所述远程计算设备而与所述远程可信消息模块交换密钥;以及

消息客户端,所述消息客户端用于:(i)将传出消息转发至所述本地可信消息模块,以及(ii)接收来自所述本地可信消息模块的传入消息,

其中,为了将传出消息安全地传输至所述远程计算设备,所述本地可信消息模块用于:(i)接收来自所述消息客户端的所述传出消息;(ii)加密所述传出消息;以及(iii)在传输至所述远程计算设备的所述远程可信消息模块之前,对所述传出消息进行密码签名;并且

其中,为了安全地接收来自所述远程计算设备的传入消息,所述本地可信消息模块用于:(i)接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息;(ii)解密所述传入消息;以及(iii)基于所述交换的密钥并在将所述传入消息传输至所述消息客户端之前验证所述传入消息的密码签名。

2.如权利要求1所述的本地计算设备,其中,用于执行对所述远程计算设备的所述证明包括用于:

从所述远程可信消息模块接收所述相应的可信执行环境的远程证明引用;以及

验证从所述远程可信消息模块接收到的所述远程证明引用。

3.如权利要求2所述的本地计算设备,其中,所述本地可信消息模块进一步用于:

生成所述本地计算设备的所述可信执行环境的本地证明引用;以及

将用于证明所述本地计算设备的所述生成的本地证明引用传输至所述远程可信消息模块。

4.如权利要求3所述的本地计算设备,其中,用于交换所述密钥包括用于:

从所述远程可信消息模块接收第一对称密钥,以用于对传输至所述远程计算设备的消息进行认证加密;

生成第二对称密钥,以用于与所述远程计算设备进行通信;以及

将所述第二对称密钥传输至所述远程可信消息模块,以用于对从所述远程计算设备传输至所述本地计算设备的消息进行认证加密。

5.如权利要求3所述的本地计算设备,其中,用于交换所述密钥包括用于:

从所述远程可信消息模块接收第一公共密钥,以用于对传输至所述远程计算设备的消息进行加密并对从所述远程计算设备接收到的已签名消息的签名进行验证;

生成密钥对,以用于与所述远程计算设备进行通信,所述密钥对包括私有密钥和第二公共密钥;

将所述第二公共密钥传输至所述可信消息模块,以用于对传输至所述远程计算设备的消息进行加密并对从所述本地计算设备接收到的已签名消息的签名进行验证。

6.如权利要求5所述的本地计算设备,其中,用于将所述传出消息安全地传输至所述远程计算设备包括用于:

由所述本地可信消息模块从所述消息客户端接收生成的消息;

由所述本地可信消息模块利用所述生成的私有密钥来对所述消息进行签名;

由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述消息进行加密;以及

由所述本地可信消息模块将所述已加密并签名的消息传输至所述远程可信消息模块。

7.如权利要求5所述的本地计算设备,其中,用于安全地接收来自所述远程计算设备的所述传入消息包括用于:

由所述本地可信消息模块接收来自所述远程可信消息模块的已加密并签名的消息;

由所述本地可信消息模块利用所述生成的私有密钥来对所述已加密并签名的消息进行解密;

由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述已加密并签名的消息的签名进行验证;以及

由所述本地可信消息模块将所述已解密并验证的消息转发至所述消息客户端。

8.如权利要求1所述的本地计算设备,其中,所述本地可信消息模块进一步用于:

判定所述远程计算设备是否已经启用所述远程可信消息模块;以及

响应于确定了所述远程可信消息模块未被启用而请求所述远程计算设备启用所述远程可信消息模块。

9.如权利要求8所述的本地计算设备,其中,用于请求所述远程计算设备启用所述远程可信消息模块包括用于:向所述远程计算设备的用户提供用于安装可信消息模块的指令。

10.如权利要求1所述的本地计算设备,其中,所述本地可信消息模块进一步用于:

从所述本地计算设备的联系人数据库中选择联系人;

对所述选择的联系人构建消息以请求在所述联系人的计算设备上启用可信消息模块;以及

将所述消息传输至所述选择的联系人的相应消息地址。

11.如权利要求10所述的本地计算设备,其中,用于请求启用所述可信消息模块包括用于:向所述选择的联系人提供用于在所述联系人的所述计算设备上安装可信消息模块的指令。

12.如权利要求1所述的本地计算设备,其中,所述本地可信消息模块进一步用于:

生成用于接收消息的私有消息接收地址;以及

通知所述远程可信消息模块将针对所述本地计算设备的消息传输至所述私有消息接收地址。

13.如权利要求12所述的本地计算设备,其中,所述本地可信消息模块进一步用于:

接收定向至所述私有消息接收地址的消息;以及

将所述接收的消息转发至所述消息客户端。

14.如权利要求13所述的本地计算设备,其中,所述本地可信消息模块进一步用于:判定定向至所述私有消息接收地址的所述消息的发送方是否被授权使用所述私有消息接收地址,

其中,用于将所述接收的消息转发至所述消息客户端包括用于:响应于确定了所述发送方被授权使用所述私有消息接收地址而将所述接收的消息转发至所述消息客户端。

15.如权利要求1至14中任一项所述的本地计算设备,其中,所述消息客户端包括以下各项之一:电子邮件客户端、即时消息传送客户端、文本消息传送客户端、图像消息传送客

户端、视频消息传送客户端或音频消息传送客户端。

16.一种用于可信消息传送的方法，所述方法包括：

由建立在本地计算设备的可信执行环境中的本地可信消息模块基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明；

由所述本地可信消息模块响应于成功证明所述远程计算设备而与所述远程可信消息模块交换密钥；以及

由所述本地可信消息模块与所述远程计算设备的所述远程可信消息模块进行通信，其中，与所述远程可信消息模块进行通信包括：将传出消息安全地传输至所述远程计算设备；或者安全地接收来自所述远程计算设备的传入消息，

其中，安全地传输所述传出消息包括：(i)接收来自所述本地计算设备的消息客户端的所述传出消息；(ii)加密所述传出消息；以及(iii)在传输至所述远程计算设备的所述远程可信消息模块之前，对所述传出消息进行密码签名，并且

其中，安全地接收传入消息包括：(i)接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息；(ii)解密所述传入消息；以及(iii)基于所述交换的密钥并且在将所述传入消息传输至所述消息客户端之前，验证所述传入消息的密码签名。

17.如权利要求16所述的方法，其中，执行对所述远程计算设备的所述证明包括：

由所述本地可信消息模块从所述远程可信消息模块接收所述相应的可信执行环境的远程证明引用；以及

由所述本地可信消息模块对从所述远程可信消息模块接收到的所述远程证明引用进行验证。

18.如权利要求17所述的方法，进一步包括：

由所述本地可信消息模块生成所述本地计算设备的所述可信执行环境的本地证明引用；以及

由所述本地可信消息模块向所述远程可信消息模块传输用于证明所述本地计算设备的所述生成的本地证明引用。

19.如权利要求18所述的方法，其中，交换所述密钥包括：

由所述本地可信消息模块从所述远程可信消息模块接收第一公共密钥，以用于对传输至所述远程计算设备的消息进行加密并对从所述远程计算设备接收到的已签名消息的签名进行验证；

由所述本地可信消息模块生成密钥对以用于与所述远程计算设备进行通信，所述密钥对包括私有密钥和第二公共密钥；

将所述第二公共密钥从所述本地可信消息模块传输至所述远程可信消息模块，以用于对传输至所述本地计算设备的消息进行加密并对从所述本地计算设备接收到的已签名消息的签名进行验证。

20.如权利要求19所述的方法，其中，将所述传出消息安全地传输至所述远程计算设备包括：

由所述本地可信消息模块从所述消息客户端接收生成的消息；

由所述本地可信消息模块利用所述生成的私有密钥来对所述消息进行签名；

由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述消息进行加密;以及

由所述本地可信消息模块将所述已加密并签名的消息传输至所述远程可信消息模块。

21.如权利要求19所述的方法,其中,安全地接收来自所述远程计算设备的所述传入消息包括:

由所述本地可信消息模块接收来自所述远程可信消息模块的已加密并签名的消息;

由所述本地可信消息模块利用所述生成的私有密钥来对所述已加密并签名的消息进行解密;

由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述已加密并签名的消息的签名进行验证;以及

由所述本地可信消息模块将所述已解密并验证的消息转发至所述消息客户端。

22.如权利要求16所述的方法,进一步包括:

由所述本地可信消息模块从所述本地计算设备的联系人数据库中选择联系人;

由所述本地可信消息模块对所述选择的联系人构件消息以请求在所述联系人的计算设备上启用可信消息模块;以及

由所述本地可信消息模块将所述消息传输至所述选择的联系人的相应消息地址。

23.如权利要求16所述的方法,进一步包括:

由所述本地可信消息模块生成用于接收消息的私有消息接收地址;以及

由所述本地可信消息模块通知所述远程可信消息模块将针对所述本地计算设备的消息传输至所述私有消息接收地址。

24.如权利要求37所述的方法,进一步包括:

由所述本地可信消息模块接收定向至所述私有消息接收地址的消息;

由所述本地可信消息模块将所述接收的消息转发至所述消息客户端;以及

由所述本地可信消息模块判定定向至所述私有消息接收地址的所述消息的发送方是否被授权使用所述私有消息接收地址,

其中,将所述接收的消息转发至所述消息客户端包括:响应于确定了所述发送方被授权使用所述私有消息接收地址而将所述接收的消息转发至所述消息客户端。

25.一种或多种机器可读存储介质,包括存储于其上的多条指令,所述指令响应于被计算设备执行而使所述计算设备执行如权利要求16至24中任一项所述的方法。

病毒式可分配可信消息传送

[0001] 相关美国专利申请的交叉引用

[0002] 本申请要求于2014年8月29日提交的题为“VIRALLY DISTRIBUTABLE TRUSTED MESSAGING(病毒式可分配可信消息传送)”的美国实用新型专利申请序列号14/473,308的优先权。

背景技术

[0003] 电子通信(如电子邮件、文本消息传送和即时消息传送)主导人们在日常基础上与彼此进行私人通信的方式。此外,电子邮件和文本消息传送经常用于传送非常机密的信息,如,网站密码重置信息以及与用户持有的各个帐户有关的信息。换句话说,那些技术在某些方面已经成为互联网的“信任根基(root oftrust)”。然而,使用例如电子邮件传输的消息可能容易被拦截、修改或重放,从而使它们非常不安全。

[0004] 各种技术已被用来保护电子消息传送技术,如电子邮件。然而,那些技术中的许多技术是用于安全管理的集中式和/或手动方法。也就是说,这些技术通常要求第三方或特定基础设施的参与,并因此采用得非常迟缓。例如,电子邮件签名(如,安全/多用途互联网邮件扩展(S/MIME))可以用来检测对电子邮件内容的修改;然而,基于互联网的S/MIME部署依赖于公共密钥基础设施(PKI),这并不容易扩展到普通用户,并具有隐私泄露风险。

附图说明

[0005] 在附图中,以示例的方式而非限制的方式来展示在本文中所描述的概念。为了说明的简单和清楚起见,在附图中所展示的元件不一定按比例绘制。在认为适当的情况下,在附图之间重复参考标号以表示相应或相似的元件。

[0006] 图1是一种用于利用病毒式可分配可信消息传送的系统的至少一个实施例的简化框图;

[0007] 图2是图1的系统的本地计算设备的环境的至少一个实施例的简化框图;

[0008] 图3是一种通过图1的系统的本地计算设备利用病毒式可分配可信消息传送的方法的至少一个实施例的简化流程图;

[0009] 图4是一种通过图1的系统的本地计算设备病毒式分配可信消息技术的方法的至少一个实施例的简化流程图;

[0010] 图5是一种通过图1的系统的本地计算设备进行证明的方法的至少一个实施例的简化流程图;

[0011] 图6是一种通过图1的系统的本地计算设备交换密钥的方法的至少一个实施例的简化流程图;

[0012] 图7是一种通过图1的系统的本地计算设备进行安全通信的方法的至少一个实施例的简化流程图;以及

[0013] 图8是一种修改图1的系统的本地计算设备的消息接收地址的方法的至少一个实施例的简化流程图。

具体实施方式

[0014] 虽然本公开的概念易于经历各种修改和替代形式，但是在附图中已经通过示例的方式来示出了其特定实施例并且将在本文中详细地对其进行描述。然而，应理解的是，不意在将公开的概念限制于所公开的特定形式，而相反，旨在覆盖与本公开和所附权利要求一致的所有修改型式、等效型式和替代型式。

[0015] 在说明书中提到的“一个实施例”、“实施例”、“说明性施例”等指示所描述的实施例可以包括特定特征、结构或特性，但每一个实施例可能或者可能不一定包括所述特定特征、结构或特性。此外，这种短语不一定指相同的实施例。此外，当关于实施例而描述了特定特征、结构或特性时，所认为的是，无论是否进行了明确描述，关于其他实施例来实现这种特征、结构或特性都在本领域技术人员的知识内。另外，应理解的是，包括在采用“至少一个A、B和C”的形式的列表中的项目可以指(A)；(B)；(C)；(A和B)；(B和C)；(A和C)；或(A、B和C)。类似地，以“A、B或C中的至少一个”的形式列出的项可以指(A)；(B)；(C)；(A和B)；(B和C)；(A和C)；或(A、B和C)。

[0016] 在一些情况下，可以在硬件、固件、软件或其任意组合中实施所公开的实施例。所公开的实施例还可以实现为一个或多个瞬态或非瞬态机器可读(例如，计算机可读)存储介质所携带或其上所存储的指令，这些指令可以由一个或多个处理器读取和执行。机器可读存储介质可以具体化为任何存储设备、机制、或用于存储或传输采用机器可读形式的信息的其他物理结构(例如，易失性或非易失性存储器、介质盘或其他介质设备)。

[0017] 在附图中，一些结构或方法特征可能以具体安排和/或顺序示出。然而，应理解的是，可以不要求这样的具体安排和/或顺序。相反，在一些实施例中，可以采用不同于在说明性图中所示出的方式和/或顺序来安排这种特征。另外，在具体的图中包括结构性特征或方法特征并不意味着暗示在所有的实施例中都需要这个特征，并且在一些实施例中，可以不包括这个特征或者这个特征可以与其他特征组合。

[0018] 现在参照图1，用于利用病毒式可分配消息传送的说明性系统100包括本地计算设备102、网络104、和一个或多个远程计算设备106。在使用中，如下面更详细讨论的，本地计算设备102可以将可信消息技术分配至远程计算设备106，所述远程计算设备进而可以进一步将可信消息传送技术分配至其他计算设备。换句话说，可信消息技术可以被本地计算设备102和/或远程计算设备106病毒式分配。另外，本地计算设备102利用消息传输协议、消息编码和密码技术来在本地计算设备102的可信消息模块与远程计算设备106的相应可信消息模块之间安全地发射和接收消息。

[0019] 本地计算设备102可以具体化为能够建立与(多个)远程计算设备106的通信链路并执行本文所描述的功能的任何类型的计算设备。例如，本地计算设备102可以具体化为台式计算机、服务器、膝上型计算机、平板计算机、笔记本、上网本、超极笔记本™、蜂窝式电话、智能电话、个人数字助理、移动互联网设备、可穿戴式计算设备、混合设备和/或任何其他计算/通信设备。如图1中所示，说明性本地计算设备102包括处理器110、输入/输出(“I/O”)子系统112、存储器114、通信电路116、数据存储设备118、一个或多个外围设备120、以及联系人数据库122。另外，在一些实施例中，本地计算设备102可以包括可信执行模块124。当然，在其他实施例中，本地计算设备102可以包括其他或附加部件，如典型计算设备中常见的那

些(例如,各种输入/输出设备和/或其他部件)。另外,在一些实施例中,这些说明性部件中的一个或多个部件可以合并在另一部件中、或能以其他方式来自另一部件的部分。例如,在一些实施例中,可以将存储器114或者其一部分结合到处理器110中。

[0020] 处理器110可以具体化为能够执行在本文中所描述的功能的任何类型的处理器。例如,处理器110可以具体化为(多个)单核或多核处理器、数字信号处理器、微控制器、或其他处理器或处理/控制电路。类似地,存储器114可以具体化为能够执行在此所述功能的任何类型的易失性或非易失性存储器或数据储存器。在运行中,存储器114可以存储在本地计算设备102运行过程中所使用的各种数据和软件,如,操作系统、应用、程序、函数库和驱动程序。存储器114经由I/O子系统112通信地耦合至处理器110,所述I/O子系统可以具体化为用于促进与本地计算设备102的处理器110、存储器114、以及其他部件的输入/输出操作的电路和/或部件。例如,I/O子系统112可以具体化为、或能以其他方式包括用于促进输入/输出操作的存储器控制器中枢、输入/输出控制中枢、固件设备、通信链路(即,点到点链路、总线链路、线、电缆、光导、印刷电路板迹线等)和/或其他部件和子系统。在一些实施例中,I/O子系统112可以形成片上系统(SoC)的一部分并且与处理器110、存储器114以及本地计算设备102的其他部件一起被整合在单个集成电路芯片上。

[0021] 本地计算设备102的通信电路116可以具体化为任何通信电路、设备或其集合,能够使本地计算设备102与其他远程设备(例如,远程计算设备106)之间的通信成为可能。通信电路116可以被配置成用于使用任何一项或多项通信技术(例如,无线或有线通信)和相关联的协议(例如,以太网、蓝牙®、Wi-Fi®、WiMAX等)来实现这种通信。

[0022] 数据存储设备118可以具体化为配置成用于对数据进行短期或长期存储的任何类型的一种或多种设备,例如,存储器设备和电路、存储卡、硬盘驱动器、固态驱动器或其他数据存储设备。数据存储设备118和/或存储器114可以在本地计算设备102的操作过程中存储各种数据,如,例如,密钥、密钥证书、和/或在如下讨论的本地计算设备102的操作中有用的其他数据。另外,在一些实施例中,联系人数据库122或其一部分可以存储在数据存储设备118中。

[0023] 在一些实施例中,本地计算设备102还可以包括一个或多个外围设备120。外围设备120可以包括任意数量的附加外围设备或接口设备,如扬声器、麦克风、附加存储设备等等。包括在外围设备120中的特定设备可以例如取决于本地计算设备102的类型和/或预期用途。

[0024] 如下面所讨论的,联系人数据库122存储本地计算设备102的用户的联系人(即,个人、企业、组织和/或其他实体)的信息。根据特定实施例,所述联系信息可以包括例如联系人姓名、物理地址、消息接收地址(例如,电子邮件地址、电话号码、即时消息传送昵称、互联网协议(IP)地址等)、和/或与联系人有关的其他信息。联系人数据库122可以是适合用于存储与联系人有关的数据的任何电子结构安排。当然,在一些实施例中,联系人数据库122可以具体化为数据库或用于存储联系人信息的合适数据结构的集合。另外,尽管说明性联系人数据库122被示出为存储在本地计算设备102上,但是在其他实施例中,联系人数据库122或其一部分可被远程地存储并且可由本地计算设备102访问(即,通过网络104)。

[0025] 可信执行模块124被配置成用于建立可信执行环境(例如,图2的可信执行模块202),以用于安全地执行指令。在一些实施例中,可信执行模块124包括本地计算设备102的

资源子集。例如，如图1所示，处理器110、I/O子系统112、存储器114、通信电路116、数据存储设备118和/或外围设备120可以包括针对可信执行模块124的资源分区（例如，专用分区）。在其它实施例中，可信执行模块124可以具体化为专用可信计算引擎，所述专用可信计算引擎例如嵌入在I/O子系统112内或以其他方式通信地耦合至I/O子系统112。应理解的是，可信执行模块124可以被建立为或以其他方式利用各种技术，包括，例如，英特尔®软件防护扩展（SGX）、可信执行引擎（TEE）、可信平台模块（TPM）、英特尔®融合安全引擎（CSE）、ARM® TrustZone®、英特尔®管理引擎、英特尔®Chaabi安全引擎、和/或用于建立安全和可信执行环境的其他技术和机制。

[0026] 网络104可以具体化为能够促进本地计算设备102与远程设备（例如，远程计算设备106）之间的通信的任何类型的通信网络。这样，网络104可以包括一个或多个网络、路由器、交换机、计算机和/或其它中间设备。例如，网络104可以具体化为或以其他方式包括一个或多个蜂窝网络、电话网络、局域网或广域网、公共可用的全球网络（例如，互联网）、自组织网络、或其任意组合。

[0027] 每个远程计算设备106可以具体化为能够执行本文所描述的功能的任何类型的计算设备。例如，在一些实施例中，远程计算设备106可以类似于如上所述的本地计算设备102。也就是说，每个远程计算设备106可以具体化为台式计算机、服务器、膝上型计算机、平板计算机、笔记本、上网本、超极笔记本™、蜂窝式电话、智能电话、个人数字助理、移动互联网设备、可穿戴式计算设备、混合设备和/或任何其他计算/通信设备。此外，远程计算设备106可以包括类似于以上讨论的本地计算设备102的那些部件的部件。对本地计算设备102的那些部件的描述同样适用于远程计算设备106的部件的描述并且为了描述的清晰性在此不再重复。此外，应理解的是，任何远程计算设备106可以包括在计算设备中常见的其它部件、子部件和设备，以上参照本地计算设备102不对其进行讨论并且为了描述的清晰性在此不进行讨论。

[0028] 现在参照图2，在使用中，本地计算设备102建立用于利用病毒式可分配可信消息传送的环境200。说明性环境200包括可信消息模块202、一个或多个消息客户端204、以及通信模块206。如下面讨论的，在本说明性实施例中，可信消息模块202建立在可信执行环境208中。另外，如所示，可信消息模块202包括病毒式传播模块（virality module）210、安全模块212、协议管理模块214和地址协调模块216。环境200的每个模块可以具体化为硬件、软件、固件或它们的组合。例如，环境200的模块、逻辑和其他部件中的每一个可以形成本地计算设备102的处理器110的一部分或以其他方式由本地计算设备102的处理器110来建立。

[0029] 如下面更详细讨论的，取决于具体实施例，可信消息模块202可以将可信消息技术病毒式分配至其他用户、执行各种安全相关的功能（例如，证明和密码术）、利用用于安全消息传输（例如，至远程计算设备106上对应的可信消息模块）的各种消息协议和编码、和/或修改本地计算设备102和/或远程计算设备106的消息接收地址。在一些实施例中，可信消息模块202可以建立在可信执行环境208中。也就是说，可信执行环境208可被建立用于确保可信消息模块202的功能是在安全且可信的环境中执行的。例如，在一些实施例中，可以使用英特尔®软件防护扩展（SGX）技术将可信执行环境208建立为安全区域。在其它实施例中，可以使用例如可信执行引擎（TEE）、可信平台模块（TPM）、英特尔®融合安全引擎（CSE）、

ARM® TrustZone®技术、和/或用于建立安全和可信执行环境的其他技术和机制建立可信执行环境208。在说明性实施例中，如以下所讨论的，本地计算设备102的可信消息模块202和/或其它模块可以对可信执行环境208进行“测量”(例如，证明引用(attestationquote))，所述“测量”可以用来确定可信执行环境208和/或建立在可信执行环境208中或在可信执行环境208中执行的模块的安全性。此外，在一些实施例中，可信执行环境208可以建立在隔离的硬件部件(例如，安全协处理器)中。

[0030] 如以上所指示的，可信消息模块202包括病毒式传播模块210、安全模块212、协议管理模块214和地址协调模块216。病毒式传播模块210处理可信消息传送技术至远程计算设备106的病毒式分配。具体地，如下面所讨论的，病毒式传播模块210可以构建并传输消息至远程计算设备106中的一个或多个用户，从而请求用户在远程计算设备106上安装或以其他方式启用可信消息传送技术(例如，相应的可信消息模块)。所述请求可以包括例如用于下载可信消息模块(例如，“应用商店”类型安装的辅助插件/实用程序)的链接和/或用于安装/启用可信消息模块的指令。根据具体实施例，病毒式传播模块210可以响应于某个状态的出现自动地生成并传输这类消息。例如，在一些实施例中，本地计算设备102可以以不安全的形式接收来自远程计算设备106的消息。在接收时，病毒式传播模块210可以请求发送远程计算设备106的用户安装或启用远程可信消息模块(例如，以便继续与本地计算设备102进行通信)。在一些实施例中，病毒式传播模块210可以搜索本地计算设备102的联系人数据库122并将这类消息传输至标识在联系人数据库122中一个或多个联系人(例如，他们中的全部)(例如，基于相应的消息地址，如，电子邮件地址)。病毒式传播模块210可以在初始启用可信消息模块202时、当新的联系人被标识时、或根据其他标准来周期性地这样操作。因此，在一些实施例中，病毒式传播模块210可以维持指示哪些远程计算设备106已启用可信消息模块、哪些已经传输请求以启用可信消息模块的记录，和/或其他相关信息。应理解的是，可信消息技术的分配在某种意义上是病毒式的，其中，当在远程计算设备106上安装或启用相应的可信消息模块时，那些设备106在与设备106的用户进行或不进行交互的情况下可以(例如，基于其相应的联系人数据库)进一步将可信消息技术分配至其他计算设备等等。

[0031] 安全模块212执行可信消息模块202的与安全发射和接收消息有关的各种安全功能。如以上所指示的，在本说明性实施例中，可信消息模块202可以在可信执行环境208中运行。因此，在这种实施例中，安全模块212可以执行本地计算设备102的证明(例如，以提供给远程计算设备106)并评估由远程计算设备106提供的证明测量(例如，证明引用)。在一些实施例中，安全模块212可以基于本地计算设备102的可信执行环境208生成证明引用。例如，安全模块212可以根据具体实施例生成SGX领域引用、TPM引用、和/或基于可信执行环境208的另一类型的信任引用。具体地，在一些实施例中，安全模块212对在可信执行环境208中执行(或用于执行)的代码进行测量(例如，求散列)，以证明在可信执行环境208中执行的代码的完整性。

[0032] 如以上所指示的，安全模块212还可以基于远程计算设备106的相应可信执行环境接收来自远程计算设备106的证明引用并验证所述证明引用。应理解的是，安全模块212可以利用任何合适的算法、技术、和/或机制来这样做。例如，在一些实施例中，安全模块212计算在其自己的可信执行环境208中执行的代码的证明引用(例如，已签名的散列)，并将所述

散列与由远程计算设备106提供的证明引用进行比较。替代性地或另外地，安全模块212可以将接收的证明引用与嵌入可信消息模块202或以其他方式由安全模块212可访问的白名单进行比较。在一些实施例中，安全模块212可以利用英特尔®Sign-and-Mac(SIGMA)技术来执行证明，并且增强隐私标识(EPID)技术可用于保护隐私(例如，SIGMA-EPID协议可用于证明和加密目的)。

[0033] 如本文所述，安全模块212被配置成执行各种加密功能，以确保可信消息模块202与远程计算设备106上的相应可信消息模块之间安全且私密的通信。在一些实施例中，安全模块212可以执行与远程计算设备106的密钥交换。例如，安全模块212可以执行迪菲-赫尔曼(Diffie-Hellman)密钥交换、和椭圆曲线迪菲-赫尔曼密钥交换、或与远程计算设备106的另一种合适的密钥交换协议(例如，以生成会话密钥)。如下面所讨论的，安全模块212生成包括公共密钥和私有密钥的密钥对并将所述公共密钥传输至远程计算设备106的相应可信消息模块以交换所述远程计算设备106的公共密钥。尽管这些技术在此主要是关于非对称密钥对(即，公共密钥和私有密钥)描述的，但是应理解的是，(多个)合适的对称密码算法可在其他实施例中被用于生成对称密钥。在这种实施例中，可以与远程计算设备106交换对称密钥，另外或替代性地，如本文所述交换非对称密钥。此外，在一些实施例中，密钥可被分层，从而使得“顶层”关系密钥可被周期性地用来保护“临时”密钥，所述临时密钥在被刷新之前用于某预定时间段，并且可以在顶层关系密钥的保护传输所述临时密钥。通过生成用于与每个远程计算设备106进行通信的单独密钥，消除了利用可信第三方进行安全验证的通信。

[0034] 应进一步理解的是，安全模块212可以生成用于数据加密并且用于对传输至远程计算设备106的数据(例如，消息)进行密码签名的各种密钥。例如，安全模块212可以使用被生成用于与特定远程计算设备106进行通信的密钥对的私有密钥来对消息进行签名。应理解的是，可以基于任何合适的算法(如，例如，Rivest-Shamir-Adleman(RSA)，椭圆曲线密码术(ECC)、数字签名算法(DSA)、或ElGamal)生成和/或利用特定的密钥。虽然本文讨论的主要涉及基于非对称加密的加密和签名，但是应进一步理解的是，可以在各实施例中利用对称加密。例如，在一些实施例中，数据本身可以是对称加密的，而对称密钥然后可以用非对称密钥进行加密并且与加密数据一起被传输。在其他实施例中，仅对称密钥用于本地计算设备102与远程计算设备106之间的安全通信。在一些实施例(如使用对称加密的那些实施例)中，代替或除了使用非对称密钥的签名认证之外，可以使用认证加密来确立可靠性。一些这种认证加密算法包括，例如，伽罗瓦/计数器模式(GCM)、偏移码本模式(OCB)、具有密码块链接消息认证码的计数器(CCM)、Encrypt-then-MAC(EtM)、和/或其他认证加密方案。应进一步理解的是，接收和/或发射的消息可以是合成对象(例如，包括文字、附件和/或其它数据结构)。因此，在一些实施例中，在签名和/或加密之前，合成消息可以被合并成有待签名和/或加密的单个对象。在其他实施例中，可以单独地对一个或多个对象进行签名/加密。此外，所述消息还可以在签名和加密之前被压缩。另外，在一些实施例中，安全模块212可以要求用户存在的证据，在这种情况下，安全模块212可以利用例如安全快速可靠登录(SQRL)和/或以其它方式提示用户提供存在证据(例如，通过输入PIN或扫描QR码)。此外，在一些实施例中，安全模块212可以生成用于传输至远程计算设备106的密钥证书。

[0035] 协议管理模块214被配置成用于利用各种消息传输协议和消息编码来将消息安全

地传输至远程计算设备106的相应可信消息模块(例如,与通信模块206合作)。例如,如图2所示,环境200可以包括用于管理本地计算设备102与远程计算设备106之间的通信的一个或多个消息客户端204。具体地,消息客户端204可以包括电子邮件客户端218(例如,使用邮局协议(POP)或互联网消息访问协议(IMAP))、即时消息传送客户端220、和/或文本消息传送客户端222(例如,使用短消息服务(SMS))。这样,在一些实施例中,可信消息模块202可以被配置成用于经由电子邮件、即时消息传送和/或文本消息传送安全地传达消息。在一些实施例中,即时消息传送客户端220被配置成用于处理互联网中继聊天(IRC)通信(例如,对等IRC)和/或基于其他即时消息传送协议的通信。

[0036] 在说明性实施例中,为了允许安全的电子邮件通信,协议管理模块214可以利用用于消息帧交换的MIME扩展机制并实现简单邮件传输协议(SMTP)和互联网消息访问协议(IMAP)服务。例如,协议管理模块214确保电子邮件消息经由SMTP外部协议(如,MIME类型和/或如美国标准信息交换码(ANSCII)编码的blob)被隧道式传输。协议管理模块214类似地确保可信消息模块202在发射和接收即时消息和文本消息时“背负(Piggyback)”适当的协议并利用适当的编码。当然,应理解的是,取决于具体的消息传送协议(例如,电子邮件消息传送与文本消息传送),可能存在对帧大小的限制以及其他约束。此外,协议管理模块214根据消息类型(例如,电子邮件、文本消息、即时消息等)确保消息在可信消息模块202与适当的消息客户端204之间进行传输。应进一步理解的是,可以采用各种其它架构来处理如本文所述的安全通信。例如,尽管可信消息模块202被描述为能够使用各种消息客户端204来处理所述通信,但是在一些实施例中,本地计算设备102可以包括针对每个消息客户端204的不同的可信消息模块202(例如,针对电子邮件客户端218而非即时消息传送客户端220的单独可信消息模块202)。

[0037] 地址协调模块216允许可信消息模块202修改远程计算设备106的消息接收地址以用于随后与远程计算设备106进行通信。例如,可能期望远程计算设备106之一通过与可信消息模块202与远程计算设备106最初通信的地址(例如,私有地址通信)不同的消息地址(例如,电子邮件地址)进行通信。在那些情况下,地址协调模块216可以用新的联系信息更新联系人数据库122和/或其他记录。应理解的是,在一些实施例中,那些变化可以与相应的消息客户端204分离。例如,在这种实施例中,用户仍可以使用旧的消息地址来构建针对远程计算设备106的用户的消息,并且地址协调模块216将在安全传输之前修改消息头部以确保其定向至更新后的地址。地址协调模块216可以类似地修改期望在其处接收来自特定远程计算设备106的消息的地址。因此,在一些实施例中,地址协调模块216被配置成用于生成在其处接收消息的新私有消息地址并且通知远程计算设备106使用所述私有消息地址来进行随后的通信。在所述私有消息地址处收到的消息随后可被转发至恰当的消息客户端(例如,如果发送方被授权使用本地计算设备102的私有消息地址)。

[0038] 通信模块206通过网络104处理本地计算设备102与远程计算设备(例如,远程计算设备106)之间的通信。如在本文中详细讨论的,通信模块206被配置成用于促进可信消息模块202与远程计算设备106的相应可信消息模块之间的安全通信。因此,通信模块206被配置成用于发射/接收往/来于远程计算设备106的各种密钥和加密通信。

[0039] 现在参照图3,在使用中,本地计算设备102可以执行一种用于利用病毒式可分配可信消息传送的方法300。如以上所指示的,本地计算设备102可以根据具体实施例使可信

消息传送技术(例如,可信消息模块202)病毒式分配至远程计算设备106、建立与远程计算设备106的可信数字关系(例如,通过证明和密码加密/签名)、通过其相应的可信消息模块与远程计算设备106进行安全通信、和/或修改计算设备102、106的各消息地址。应理解的是,在其他实施例中,本文描述的特征可以按与本文呈现的顺序不同的顺序发生。例如,在一些实施例中,方法300的病毒式分配特征和/或消息地址修改可以按完全不同的顺序发生。

[0040] 说明性方法300始于框302,其中,本地计算设备102如果尚未启用可信消息模块202则可以这样做。例如,在一些实施例中,本地计算设备102可能已经接收到来自远程计算设备106的用于安装或以其他方式启用可信消息模块202的请求。在其它实施例中,可信消息模块202可以在启动本地计算设备102时被启用或被持久启用。应理解的是,在本说明性实施例中,本地计算设备102的可信消息模块202在被启用之后(即,如果尚未启用的话)执行方法300。在框304中,本地计算设备102可以病毒式分配可信消息技术。换句话说,本地计算设备102可以征求其他计算设备(例如,远程计算设备106)来安装或以其他方式启用相应的可信消息模块。

[0041] 这样做,本地计算设备102可以执行如图4所述的方法400。更具体地,在本说明性实施例中,方法400是由本地计算设备102的可信消息模块202执行的。方法400始于框402,其中,本地计算设备102判定是否分配可信消息技术。若是,则本地计算设备102从联系人数据库122中选择“下一个”联系人。如以上所讨论的,在本说明性实施例中,联系人数据库122包括本地计算设备102的用户已知的一组联系人和/或实体以及那些人的相应消息地址。在本说明性实施例中,本地计算设备102选择联系人并标识与所述联系人相关联的电子邮件地址。在其他实施例中,本地计算设备102可以标识与不同消息客户端204相关联的消息地址并执行本文所述的功能。应理解的是,构成“下一个”联系人的联系人可以根据具体实施例而变化。在本说明性实施例中,下一个联系人是本地计算设备102尚未向其传输征求启用可信消息模块的消息的任何联系人。在一些实施例中,本地计算设备102的用户可以选择向其分配可信消息技术(例如,用户想要利用其在密码保护下进行安全通信的那些技术)的特定联系人。

[0042] 在框406中,本地计算设备102构建针对所选联系人的消息以请求在所述联系人的相应计算设备上启用可信消息模块。在这样做时,在框408中,本地计算设备102可以包括用于安装所述可信消息模块的链接和指令。例如,邀请信息或请求可以包括针对允许远程用户轻易地安装可信消息模块(例如,复制“应用商店”安装环境)的辅助插件/实用程序的链接。在一些实施例中,消息还可以指示本地计算设备102的用户不愿继续与远程用户进行通信,除非远程用户安装用于安全通信的可信消息模块。在框410中,本地计算设备102将所述构建的消息传输至在所选联系人的相应消息地址处的联系人,从而使得远程用户可以安装或以其他方式启用可信消息模块以进行安全通信。应理解的是,在一些实施例中,邀请消息可以包括本文所描述的密钥交换协议的第一部分。例如,本地计算设备102可以生成用于与所选联系人的远程计算设备106一起使用的密钥对并利用所述邀请将所述密钥对的公共密钥传输至远程计算设备106。如果远程计算设备106的用户确定安装/启用可信消息技术,则远程计算设备106可以生成其自己的密钥对并将所述公共密钥传输至本地计算设备102,如下所述。

[0043] 在框412中，本地计算设备102判定联系人数据库122中是否存在要向其发送邀请消息或以其它方式征求安装/启用可信消息模块的任何剩余附加联系人。如以上所指示的，在一些实施例中，本地计算设备102维持已经启用了可信消息模块的远程计算设备106和/或联系人的记录。在一些实施例中，所述记录还可以包括关于密钥交换的当前状态的信息，包括，例如，密钥交换的中间结果、用于再调用密钥交换的状态的注释、和/或与密钥交换相关的其它信息。通过这样做，本地计算设备102能够确定哪些远程计算设备106准备好进行安全通信和/或哪个远程计算设备106避免征求安装可信消息传送技术。如果联系人数据库122中存在尚未被请求启用可信消息模块的剩余联系人，则方法400返回至框404，其中，本地计算设备102从联系人数据库122中选择下一个联系人。如以上所指示的，在一些实施例中，本地计算设备102可以周期性地确定病毒式分配可信消息技术，或者可以监测联系人数据库122以标识向其发送邀请消息的新添加的联系人。在一些实施例中，本地计算设备102的用户还可以手动确定以请求安装/启用来自特定联系人的可信消息技术。例如，用户可以将邀请传输至她自己，从而使得她可以在不同的计算设备上安装可信消息模块。

[0044] 返回参照图3，在框306中，本地计算设备102判定是否在远程计算设备106上启用了可信消息模块。例如，可信消息模块202可能希望建立本地计算设备102的可信消息模块202与远程计算设备106的相应可信消息模块之间的可信关系。在另一个实施例中，本地计算设备102可能已经接收到来自消息客户端204之一的消息，并且可能需要判定在其中传输消息的相应可信消息模块是否存在。替代性地，可能已经由已经以不安全方式(例如，仅通过消息客户端204)从远程计算设备106接收到消息的本地计算设备102促进查询。在任何情况下，如果本地计算设备102确定未启用远程计算设备106上的可信消息模块，则本地计算设备102可以请求远程计算设备106来安装或以其它方式启用可信消息模块，如上所述。

[0045] 在框310中，本地计算设备102建立与远程计算设备106的可信消息模块的可信关系。更具体地，本地计算设备102的可信消息模块202(即，本地可信消息模块)建立与远程计算设备106(即，远程可信消息模块)的相应可信消息模块的可信关系。这样做，在本说明性实施例中，本地计算设备102可以在框312中执行对可信消息模块的证明(参见图5)，并在框314中与远程计算设备106交换公共密钥(参照图6)。在其他实施例中，本地计算设备102可以采用其他技术来建立相应的可信消息模块之间的可信关系。

[0046] 为了执行可信消息模块的证明，本地计算设备102可以执行如图5中所示的方法500。在一些实施例中，通过使用密码散列算法和/或其他合适的编码方案将可信消息模块202的已知良好图象的白名单与可信消息模块202的实际图像进行比较来证明可信消息模块202。应理解的是，白名单图像技术不受中间人攻击(例如，修改电子邮件地址以及将消息重新路由到数字关系中的其他非参与者(即，除了本地计算设备102和远程计算设备106之外的设备)影响。如以上所讨论的，在本说明性实施例中，本地计算设备102的可信消息模块202具体地执行方法500。说明性方法500始于框502，其中，本地计算设备102判定是否证明本地计算设备102与远程计算设备106。若是，则在框304中，本地计算设备102可以将消息传输至远程计算设备106，以请求所述远程计算设备106执行证明。如以上所讨论，在一些实施例中，可以使用英特尔®SIGMA技术和EPID完成所述证明。在本说明性实施例中，远程计算设备106生成远程可信消息模块和/或在其中执行与远程可信消息模块相关联的代码的可信执行环境的证明引用。如以上所讨论的，远程计算设备106可以根据具体实施例生成SGX

领域引用、TPM引用、和/或基于远程计算设备106的可信执行环境的另一类型的信任引用。在这样做时，远程计算设备106可以对在其可信执行环境中执行(或用于执行)的代码进行测量(例如，求签名散列)。

[0047] 在框506中，本地计算设备102接收来自远程计算设备106的证明引用。在框508中，本地计算设备102生成本地计算设备102的证明引用以便向远程计算设备106证明其完整性。在本说明性实施例中，本地计算设备102的证明引用可以以与上述远程计算设备106的证明引用类似的方式生成。在框510中，本地计算设备102验证远程计算设备106的证明引用。应理解的是，本地计算设备102可以利用任何合适的技术、算法和/或机制这样做。例如，在一些实施例中，本地计算设备102将基于其自己的可信执行环境208生成的证明引用与从远程计算设备106接收到的远程证明引用进行比较，以判定它们是否匹配(即，正在执行或有待执行的代码在由证明算法确定为重要的方面是否相同)。在一些实施例中，本地计算设备102将远程证明引用与存储在本地计算设备102上的白名单进行比较，以确定远程可信消息模块是否可靠。

[0048] 在框512中，本地计算设备102将本地可信消息模块202和/或可信执行环境208的生成的证明引用传输至远程计算设备106以由远程计算设备106进行验证。在框516中，本地计算设备102判定本地计算设备102与远程计算设备106的证明是否成功。若否，则方法500可以返回至框502，其中，本地计算设备102再次尝试证明计算设备102、106。

[0049] 为了交换密钥，本地计算设备102可以执行图6的方法600。如以上所讨论的，在本说明性实施例中，本地计算设备102的可信消息模块202执行方法600。说明性方法600始于框602，其中，本地计算设备102判定是否交换密钥。若是，则在框604中，本地计算设备102接收来自远程计算设备106的公共密钥，以用于对传输至远程计算设备106的消息进行加密。另外，如以上所讨论的，公共密钥还可用于验证从远程计算设备106接收的消息的签名。这样，在一些实施例中，相同的公共密钥可以用作双重目的。应理解的是，在一些实施例中，远程计算设备106可以响应于成功证明本地计算设备102生成包括发射的公共密钥以及相应的私有密钥的密钥对。私有密钥可以例如用于对远程计算设备106的传出消息进行图形加密签名。如以上所讨论的，可以利用对称密钥，另外或替代性地，可以利用非对称密钥(例如，使用认证加密)。

[0050] 在框606中，本地计算设备102生成密钥对，以用于与远程计算设备106进行通信。也就是说，本地计算设备102可以生成包括公共密钥和私有密钥的密钥对。在框608中，本地计算设备102的公共密钥被传输至远程计算设备106，从而使得远程计算设备106可以利用密钥来验证由本地计算设备102传输的消息的签名和/或对有待传输至本地计算设备102的消息进行加密。

[0051] 为了便于讨论，由本地计算设备102生成的密钥对在本文中可被称作“本地”密钥对，所述“本地”密钥对包括本地公共密钥和本地私有密钥。并且，由远程计算设备106生成的密钥对在本文中可被称作“远程”密钥对，所述“远程”密钥对包括远程公共密钥和远程私有密钥。另外，应理解的是，在本说明性实施例中，本地计算设备102针对每个远程计算设备106交换一组独立的密钥，并且远程计算设备106也这样做。例如，用于本地计算设备102与第一远程计算设备106之间的通信的密钥不同于用于本地计算设备102与第二远程计算设备106之间的通信的密钥。因此，在本说明性实施例中，参照特定远程计算设备106，本地私

有密钥被本地计算设备102用来对至远程计算设备106的传出消息进行签名。另外，由于远程计算设备106利用本地公共密钥来对至本地计算设备102的传出消息进行加密，所以在本说明性实施例中，本地计算设备102还使用本地私有密钥来对那些传入的已加密并签名的消息进行解密。

[0052] 本地计算设备102还通过使用从远程计算设备106接收到的远程公共密钥来对所述图形加密签名的通信进行验证(即，验证签名)。如以上所指示的，为了在计算设备102、106之间安全地交换密钥，根据特定消息客户端204通过适当的消息协议(例如，SMTP)隧道式传输通信并且恰当地编码所述通信(例如，作为MIME类型)。另外，在一些实施例中，本地计算设备102和/或远程计算设备106可以利用各种密钥证书来安全地交换密钥。当然，所生成的和发射/接收的密钥可以存储在各自的计算设备102、106中以用于相应可信消息模块之间的随后的安全通信。例如，密钥可以被存储，其方式使得它们被映射到与计算设备102、106相关联的合适联系人和/或以其他方式与相应的(多个)消息地址进行关联。在一些实施例中，相同的密钥可以用于不同消息客户端204之间的通信(例如，电子邮件和即时消息传送)，而在其他实施例中，计算设备102、106可以根据特定的消息客户端204和/或相关特性(例如，根据特定的传输协议、消息编码、帧大小等等)生成单独的密钥。

[0053] 返回参照图3，在框316中，本地计算设备102可以在建立可信关系之后(即，由“波浪号”符号表示)在某一时刻与远程计算设备106(即，与本地计算设备102建立了可信关系的远程计算设备106)进行安全通信。换句话说，计算设备102、106可以借助其相应的可信消息模块利用生成的和交换的密钥来与彼此进行安全通信。这样做，本地计算设备102可以执行以下讨论的图7的方法700。另外，在框318中，本地计算设备102可以修改本地计算设备102的消息接收地址(即，请求远程计算设备106未来使用不同的消息地址来联系本地计算设备102)和/或在本地计算设备102上修改远程计算设备106的消息地址(例如，响应于来自远程计算设备106的请求)。应理解的是，计算设备102、106可与彼此安全通信以便进行这种修改(例如，以防止私有消息传送地址泄露给对手)。这样做，本地计算设备102可以执行以下讨论的图8的方法800。

[0054] 如以上所指示的，为了与本地计算设备102已经同其建立了可信关系的远程计算设备106安全地通信，本地计算设备进行通信102或更具体地可信消息模块202可以执行图7的方法700。如先前所讨论的，通过通信中的计算设备102、106的相应可信消息模块传达消息，而不是直接将所述消息发送至接收方的相应消息客户端或处理程序。例如，在说明性实施例中，电子邮件可以被传输至接收方的可信消息模块，而不是直接发送至SMTP服务器。说明性方法700始于框702，其中，可信消息模块202判定是否与远程计算设备106(即，与相应的可信消息模块)安全通信。若是，则可信消息模块202在框704中判定是否发射消息并且在框706中判定是否接收消息。应理解的是，在本说明性实施例中，可信消息模块是否发射或接收消息是由可信消息模块202是否已经接收到来自消息客户端204的传出消息或来自远程可信消息模块的传入消息来指定的。

[0055] 如果可信消息模块202确定发射消息，则可信消息模块202在框708中从本地计算设备102的消息客户端204接收生成的消息，如上所述。即，消息是由消息客户端204转发至或以其它方式被可信消息模块202截获以用于安全传输，而不是直接地或通过例如云中的SMTP服务将传出消息传达至远程计算设备106。在一些实施例中，可信消息模块202建立其

自身与消息客户端204之间的可靠绑定。例如，可信消息模块202可以利用本地计算设备102的操作系统中的可信绑定服务、基于超管理器的绑定程序、或者在可信执行环境208中(例如，在英特尔SGX领域中)运行的绑定服务。通过这样做，可信消息模块202确保抑制本地计算设备102上执行的恶意软件篡改可信消息模块202中用于执行例如中间人攻击的代码。在一些实施例中，绑定服务还可以将本地计算设备102的其他部件(例如，外围设备120)和/或在本地计算设备102上执行的创建上下文信息的应用程序同本地计算设备102的可信消息模块202与远程计算设备106的相应可信消息模块之间的数字关系绑定进行关联。所述上下文信息可以根据具体实施例在任何时间点在设备102和106之间进行交换。

[0056] 在框710中，可信消息模块202利用针对与远程计算设备106进行通信所生成的密钥对中的私有密钥(例如，以上讨论的本地私有密钥)来对消息进行密码签名。另外，在框712中，可信消息模块202利用从远程计算设备106接收到的公共密钥(例如，以上讨论的远程公共密钥)对消息进行加密。如以上所讨论的，可信消息模块202可以使用任何合适的技术和/或机制来标识适当的密钥。例如，在一些实施例中，可信消息模块202可将每个消息地址映射到适当的密钥(即，如果已经建立了可信关系的话)。应进一步理解的是，在一些实施例中，可信消息模块202可以在对消息进行签名之前对消息进行加密。另外，在一些实施例中，可信消息模块202还可以生成或以其他方式利用用于传输至远程计算设备106的密钥证书(例如，EPID密钥证书)来验证签名。在框714中，可信消息模块202将加密且签名的消息传输至远程计算设备106的相应可信消息模块。

[0057] 如果可信消息模块202确定接收消息，则可信消息模块202从远程计算设备106的相应可信消息模块接收加密的且加密签名的消息。换句话说，如上所述，来自远程计算设备106的可信消息模块的传入消息被定向到可信消息模块202。在框718中，可信消息模块202利用针对与远程计算设备106的通信生成的密钥对中的私有密钥(例如，以上讨论的本地私有密钥)来对加密消息进行解密。另外，在框720中，可信消息模块202利用从远程计算设备106接收到的公共密钥(例如，以上讨论的远程公共密钥)对消息的签名进行验证。应理解的是，在一些实施例中，可信消息模块202可以在解密消息之前对加密且签名的消息的签名进行验证。在框722中，可信消息模块202将经验证的消息转发至适当的消息客户端204。也就是说，在本说明性实施例中，如果消息被成功解密并且签名是有效的，则可信消息模块202将所述解密的消息转发至适当的消息客户端204。例如，如果消息是电子邮件通信，则所述消息被转发至本地计算设备102的电子邮件客户端218。在一些实施例中，可信消息模块202可以在框724中根据例如用户的系统通知偏好通知与安全通信相关的用户。例如，可信消息模块202可以通知用户所接收的消息在已被安全传输之后已经被解密且被验证。当然，可信消息模块202可以类似地通知用户消息已在何时被安全地传输和/或关于与可信消息传送技术的操作相关联的各种其他状态。

[0058] 如上所述，本地计算设备102或者更具体地可信消息模块202可以通过执行图8的方法800来修改本地计算设备102的消息接收地址。说明性方法800始于框802，其中，本地计算设备102判定是否修改本地计算设备102的消息接收地址。例如，在一些实施例中，本地计算设备102可为某些远程计算设备106提供本地计算设备102的私有消息地址，以确保本地计算设备102的用户接收和/或读取消息。

[0059] 如果本地计算设备102确定修改消息接收地址，则本地计算设备102在框804中生

成私有消息接收地址。例如，本地计算设备102可以生成期望在其处接收来自特定的(或所有的)远程计算设备106的后续电子邮件消息的新电子邮件地址。应理解的是，本地计算设备102可以使用任何合适的算法、技术、和/或机制生成私有消息接收地址。另外，尽管消息地址在本文被描述为是被生成的，但是应理解的是，在一些实施例中，本地计算设备102可以从一组预先生成的或以其他方式预先确定的消息地址中选择私有消息接收地址。

[0060] 在框806中，本地计算设备102(例如，经由远程计算设备106的相应可信消息模块)将所述生成的私有消息接收地址通知给远程计算设备106。例如，本地计算设备102可以通知远程计算设备106联系本地计算设备102的用户的新消息地址，并指示所述新消息地址将确保消息被接收和读取。例如，在一些实施例中，本地计算设备102可以具有拒绝在原始消息地址处接收某些消息(例如，具有特定类型、大小、发送方、频率等的消息)的安全策略。如以上所讨论的，远程计算设备106可以利用新消息地址更新其联系人数据库，从而使得远程可信消息模块可以例如修改定向到本地计算设备102的任何传出消息的消息头部，以反映本地计算设备102的私有消息接收地址或以其他方式确保消息被发送至正确的位置。

[0061] 在框808中，本地计算设备102判定是否已经接收到定向至私有消息接收地址的消息。例如，在一些实施例中，可信消息模块202可以接收来自远程计算设备106的相应可信消息模块的消息，并读取所述消息头部或以其他方式确定所述消息被定向到所生成的私有消息接收地址。若是，则本地计算设备102可以在框810中判定远程计算设备106(即，发送方)是否被授权使用私有消息接收地址来与本地计算设备102进行通信。例如，在一些实施例中，本地计算设备102维持其已经生成哪些私有消息接收地址的记录，并且针对那些消息地址中的每个消息地址，哪些远程计算设备106被授权通过所述消息地址来与本地计算设备102进行通信。如果远程计算设备106未被授权经由所述消息地址进行通信，则本地计算设备102可以执行任何合适的误差处理功能(例如，丢弃消息分组、通知本地计算设备102和/或远程计算设备106的用户、和/或执行另一种合适的功能)。然而，如果远程计算设备106被授权使用私有消息接收地址或者本地计算设备102不具有这样的标准，则可信消息模块202在框812中将所述消息转发至适当的消息客户端204。当然，在一些实施例中，本地计算设备102还可以(例如，响应于来自远程计算设备106的请求)在本地计算设备102上修改远程计算设备106的消息接收地址，如上所述。

[0062] 示例

[0063] 以下提供了在本文中所公开的技术的说明性示例。所述技术的实施例可以包括以下所描述的示例中的任何一个或多个示例或者其任何组合。

[0064] 示例1包括一种用于可信消息传送的本地计算设备，所述本地计算设备包括：本地可信消息模块，所述本地可信消息模块建立在可信执行环境中，用于：(i)基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明；以及(ii)响应于成功证明所述远程计算设备而与所述远程可信消息模块交换密钥；以及消息客户端，所述消息客户端用于：(i)将传出消息转发至所述本地可信消息模块；以及(ii)接收来自所述本地可信消息模块的传入消息，其中，为了将传出消息安全地传输至所述远程计算设备，所述本地可信消息模块用于：(i)接收来自所述消息客户端的所述传出消息；(ii)加密所述传出消息；以及(iii)在传输至所述远程计算设备的所述远程可信消息模块之前对所述传出消息进行密码签名；并且其中，为了安全地接收来自所述远程

计算设备的传入消息，所述本地可信消息模块用于：(i)接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息；(ii)解密所述传入消息；以及(iii)基于所述交换的密钥并在将所述传入消息传输至所述消息客户端之前验证所述传入消息的密码签名。

[0065] 示例2包括如示例1所述的主题，并且其中，用于执行对所述远程计算设备的所述证明包括用于：接收所述远程可信消息模块接收所述相应的可信执行环境的远程证明引用；以及验证从所述远程可信消息模块接收到的所述远程证明引用。

[0066] 示例3包括如示例1和2中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：生成所述本地计算设备的所述可信执行环境的本地证明引用；以及将用于证明所述本地计算设备的所述生成的本地证明引用传输至所述远程可信消息模块。

[0067] 示例4包括如示例1至3中任一项所述的主题，并且其中，用于交换所述密钥包括用于：从所述远程可信消息模块接收第一对称密钥，以用于对传输至所述远程计算设备的消息进行认证加密；生成第二对称密钥，以用于与所述远程计算设备进行通信；以及将所述第二对称密钥传输至所述远程可信消息模块，以用于对从所述远程计算设备传输至所述本地计算设备的消息进行认证加密。

[0068] 示例5包括如示例1至4中任一项所述的主题，并且其中，用于交换所述密钥包括用于：从所述远程可信消息模块接收第一公共密钥，用于对传输至所述远程计算设备的消息进行加密并对从所述远程计算设备接收到的已签名消息的签名进行验证；生成密钥对，以用于与所述远程计算设备进行通信，所述密钥对包括私有密钥和第二公共密钥；将所述第二公共密钥传输至所述远程可信消息模块，以用于对传输至所述远程计算设备的消息进行加密并对从所述本地计算设备接收到的已签名消息的签名进行验证。

[0069] 示例6包括如示例1至5中任一项所述的主题，并且其中，用于将所述传出消息安全地传输至所述远程计算设备包括用于：由所述本地可信消息模块从所述消息客户端接收生成的消息；由所述本地可信消息模块利用所述生成的私有密钥来对所述消息进行签名；由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述消息进行加密；以及由所述本地可信消息模块将所述已加密并签名的消息传输至所述远程可信消息模块。

[0070] 示例7包括如示例1至6中任一项所述的主题，并且进一步包括：将所述生成的消息的所有部分合并成封装消息；其中，用于对所述消息进行签名包括用于对所述封装消息进行签名；并且其中，用于对所述消息进行加密包括用于对所述封装消息进行加密。

[0071] 示例8包括如示例1至7中任一项所述的主题，并且其中，用于合并所述生成的消息的所述部分进一步包括：用于压缩所述生成的消息。

[0072] 示例9包括如示例1至8中任一项所述的主题，并且其中，用于安全地接收来自所述远程计算设备的所述传入消息包括用于：由所述本地可信消息模块接收来自所述远程可信消息模块的已加密并签名的消息；由所述本地可信消息模块利用所述生成的私有密钥来对所述已加密并签名的消息进行解密；由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述已加密并签名的消息的签名进行验证；以及由所述本地可信消息模块将所述已解密并验证的消息转发至所述消息客户端。

[0073] 示例10包括如示例1至9中任一项所述的主题，并且进一步包括将所述已解密并验证的消息解封装成组成部分；其中，用于转发所述已解密并验证的消息包括用于：转发所述

组成部分。

[0074] 示例11包括如示例1至10中任一项所述的主题，并且其中，用于对所述已解密并验证的消息进行解封装进一步包括用于：对所述已解密并验证的消息进行解压缩。

[0075] 示例12包括如示例1至11中任一项所述的主题，并且其中，所述消息客户端包括以下各项之一：电子邮件客户端、即时消息传送客户端、文本消息传送客户端、图像消息传送客户端、视频消息传送客户端或音频消息传送客户端。

[0076] 示例13包括如示例1至12中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：判定所述远程计算设备是否已经启用所述远程可信消息模块；以及响应于确定了所述远程可信消息模块未被启用而请求所述远程计算设备启用所述远程可信消息模块。

[0077] 示例14包括如示例1至13中任一项所述的主题，并且其中，用于请求所述远程计算设备启用所述远程可信消息模块包括用于：向所述远程计算设备的用户提供用于安装可信消息模块的指令。

[0078] 示例15包括如示例1至14中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：从所述本地计算设备的联系人数据库中选择联系人；对所述选择的联系人构建消息以请求在所述联系人的计算设备上启用可信消息模块；以及将所述消息传输至所述选择的联系人的相应消息地址。

[0079] 示例16包括如示例1至15中任一项所述的主题，并且其中，用于请求启用所述可信消息模块包括用于：向所述选择的联系人提供用于在所述联系人的所述计算设备上安装可信消息模块的指令。

[0080] 示例17包括如示例1至16中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：生成用于接收消息的私有消息接收地址；以及通知所述远程可信消息模块将针对所述本地计算设备的消息传输至所述私有消息接收地址。

[0081] 示例18包括如示例1至17中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：接收定向至所述私有消息接收地址的消息；以及将所述接收的消息转发至所述消息客户端。

[0082] 示例19包括如示例1至18中任一项所述的主题，并且其中，所述本地可信消息模块进一步用于：判定定向至所述私有消息接收地址的所述消息的发送方是否被授权使用所述私有消息接收地址，其中，用于将所述接收的消息转发至所述消息客户端包括用于：响应于确定了所述发送方被授权使用所述私有消息接收地址而将所述接收的消息转发至所述消息客户端。

[0083] 示例20包括一种用于可信消息传送的方法，所述方法包括：由建立在本地计算设备的可信执行环境中的本地可信消息模块基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明；由所述本地可信消息模块响应于成功证明所述远程计算设备而与所述远程可信消息模块交换密钥；以及由所述本地可信消息模块与所述远程计算设备的所述远程可信消息模块进行通信，其中，与所述远程可信消息模块进行通信包括将传出消息安全地传输至所述远程计算设备或者安全地接收来自所述远程计算设备的传入消息，其中，安全地传输所述传出消息包括：(i)接收来自所述本地计算设备的消息客户端的所述传出消息；(ii)加密所述传出消息；以及

(iii)在传输至所述远程计算设备的所述远程可信消息模块之前对所述传出消息进行密码签名，并且其中，安全地接收传入消息包括：(i)接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息；(ii)解密所述传入消息；以及(iii)基于所述交换的密钥并在将所述传入消息传输至所述消息客户端之前验证所述传入消息的密码签名。

[0084] 示例21包括如示例20所述的主题，并且进一步包括：由所述本地计算设备启用所述本地计算设备上的所述本地可信消息模块。

[0085] 示例22包括如示例20和21中任一项所述的主题，并且其中，执行对所述远程计算设备的所述证明包括：由所述本地可信消息模块从所述远程可信消息模块接收所述相应的可信执行环境的远程证明引用；以及由所述本地可信消息模块对从所述远程可信消息模块接收到的所述远程证明引用进行验证。

[0086] 示例23包括如示例20至22中任一项所述的主题，并且进一步包括：由所述本地可信消息模块生成所述本地计算设备的所述可信执行环境的本地证明引用；以及由所述本地可信消息模块向所述远程可信消息模块传输用于证明所述本地计算设备的所述生成的本地证明引用。

[0087] 示例24包括如示例20至23中任一项所述的主题，并且其中，交换所述密钥包括：由所述本地可信消息模块从所述远程可信消息模块接收第一公共密钥，以用于对传输至所述远程计算设备的消息进行认证加密；由所述本地可信消息模块生成第二对称密钥，以用于与所述远程计算设备进行通信；以及将所述第二对称密钥从所述本地可信消息模块传输至所述远程可信消息模块，以用于对从所述远程计算设备传输至所述本地计算设备的消息进行认证加密。

[0088] 示例25包括如示例20至24中任一项所述的主题，并且其中，交换所述密钥包括：由所述本地可信消息模块从所述远程可信消息模块接收第一公共密钥，以用于对传输至所述远程计算设备的消息进行加密并对从所述远程计算设备接收到的已签名消息的签名进行验证；由所述本地可信消息模块生成密钥对，以用于与所述远程计算设备进行通信，所述密钥对包括私有密钥和第二公共密钥；将所述第二公共密钥从所述本地可信消息模块传输至所述远程可信消息模块，以用于对传输至所述本地计算设备的消息进行加密并对从所述本地计算设备接收到的已签名消息的签名进行验证。

[0089] 示例26包括如示例20至25中任一项所述的主题，并且其中，将所述传出消息安全地传输至所述远程计算设备包括：由所述本地可信消息模块从所述消息客户端接收生成的消息；由所述本地可信消息模块利用所述生成的私有密钥来对所述消息进行签名；由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述消息进行加密；以及由所述本地可信消息模块将所述已加密并签名的消息传输至所述远程可信消息模块。

[0090] 示例27包括如示例20至26中任一项所述的主题，并且进一步包括：将所述生成的消息的所有部分合并成封装消息，其中，对所述消息进行签名包括对所述封装消息进行签名；以及对所述消息进行加密包括对所述封装消息进行加密。

[0091] 示例28包括如示例20至27中任一项所述的主题，并且其中，合并所述生成的消息的所述部分进一步包括压缩所述生成的消息。

[0092] 示例29包括如示例20至28中任一项所述的主题，并且其中，安全地接收来自所述

远程计算设备的所述传入消息包括：由所述本地可信消息模块接收来自所述远程可信消息模块的已加密并签名的消息；由所述本地可信消息模块利用所述生成的私有密钥来对所述已加密并签名的消息进行解密；由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述已加密并签名的消息的签名进行验证；以及由所述本地可信消息模块将所述已解密并验证的消息转发至所述消息客户端。

[0093] 示例30包括如示例20至29中任一项所述的主题，并且进一步包括将所述已解密并验证的消息解封装成组成部分；其中，转发所述已解密并验证的消息包括转发所述组成部分。

[0094] 示例31包括如示例20至30中任一项所述的主题，并且其中，对所述已解密并验证的消息进行解封装进一步包括对所述已解密并验证的消息进行解压缩。

[0095] 示例32包括如示例20至31中任一项所述的主题，并且其中，所述消息客户端包括以下各项之一：电子邮件客户端、即时消息传送客户端、文本消息传送客户端、图像消息传送客户端、视频消息传送客户端或音频消息传送客户端之一。

[0096] 示例33包括如示例20至32中任一项所述的主题，并且进一步包括：由所述本地可信消息模块判定所述远程计算设备是否已经启用所述远程可信消息模块；以及由所述本地可信消息模块响应于确定了所述远程可信消息模块未被启用而请求所述远程计算设备启用所述远程可信消息模块。

[0097] 示例34包括如示例20至33中任一项所述的主题，并且其中，请求所述远程计算设备启用所述远程可信消息模块包括：向所述远程计算设备的用户提供用于安装可信消息模块的指令。

[0098] 示例35包括如示例20至34中任一项所述的主题，并且进一步包括：由所述本地可信消息模块从所述本地计算设备的联系人数据库中选择联系人；由所述本地可信消息模块对所述选择的联系人构建消息以请求在所述联系人的计算设备上启用可信消息模块；以及由所述本地可信消息模块将所述消息传输至所述选择的联系人的相应消息地址。

[0099] 示例36包括如示例20至35中任一项所述的主题，并且其中，请求启用所述可信消息模块包括：向所述选择的联系人提供用于在所述联系人的所述计算设备上安装可信消息模块的指令。

[0100] 示例37包括如示例20至36中任一项所述的主题，并且进一步包括：由所述本地可信消息模块生成用于接收消息的私有消息接收地址；以及由所述本地可信消息模块通知所述远程可信消息模块将针对所述本地计算设备的消息传输至所述私有消息接收地址，

[0101] 示例38包括如示例20至37中任一项所述的主题，并且进一步包括：由所述本地可信消息模块接收定向至所述私有消息接收地址的消息；以及由所述本地可信消息模块将所述接收的消息转发至所述消息客户端。

[0102] 示例39包括如示例20至38中任一项所述的主题，并且进一步包括：由所述本地可信消息模块判定定向至所述私有消息接收地址的所述消息的发送方是否被授权使用所述私有消息接收地址，其中，将所述接收的消息转发至所述消息客户端包括：响应于确定了所述发送方被授权使用所述私有消息接收地址而将所述接收的消息转发至所述消息客户端。

[0103] 示例40包括一种计算设备，所述计算设备包括：处理器；以及存储器，所述存储器具有存储于其中的多条指令，所述指令当由所述处理器执行时使所述计算设备执行如示例

20至39中任一项所述的方法。

[0104] 示例41包括一种或多种机器可读存储介质，包括存储于其上的多条指令，所述指令响应于被计算设备执行而使所述计算设备执行如示例20至39中任一项所述的方法。

[0105] 示例42包括一种用于可信消息传送的本地计算设备，所述本地计算设备包括：用于由建立在所述本地计算设备的可信执行环境中的本地可信消息模块基于与建立在远程计算设备的可信执行环境中的相应远程可信消息模块进行的通信来执行对所述远程计算设备的证明的装置；用于由所述本地可信消息模块响应于成功证明所述远程计算设备而与所述远程可信消息模块交换密钥的装置；以及用于由所述本地可信消息模块与所述远程计算设备的所述远程可信消息模块进行通信的装置，其中，所述用于与所述远程可信消息模块进行通信的装置包括用于将传出消息安全地传输至所述远程计算设备的装置或者用于安全地接收来自所述远程计算设备的传入消息的装置，其中，所述用于安全地传输所述传出消息的装置包括：(i)用于接收来自所述本地计算设备的消息客户端的所述传出消息的装置；(ii)用于加密所述传出消息的装置；以及(iii)用于被传输至所述远程计算设备的所述远程可信消息模块之前对所述传出消息进行密码签名的装置，并且其中，所述用于安全地接收传入消息的装置包括：(i)用于接收来自所述远程计算设备的所述远程可信消息模块的所述传入消息的装置；(ii)用于解密所述传入消息的装置；以及(iii)用于基于所述交换的密钥并在将所述传入消息传输至所述消息客户端之前验证所述传入消息的密码签名的装置

[0106] 示例43包括如示例42所述的主题，并且进一步包括：用于启用所述本地计算设备上的所述本地可信消息模块的装置。

[0107] 示例44包括如示例42和43中任一项所述的主题，并且其中，所述用于执行对所述远程计算设备的所述证明的装置包括：用于由所述本地可信消息模块从所述远程可信消息模块接收所述相应的可信执行环境的远程证明引用的装置；以及用于由所述本地可信消息模块对从所述远程可信消息模块接收到的所述远程证明引用进行验证的装置。

[0108] 示例45包括如示例42至44中任一项所述的主题，并且进一步包括：用于由所述本地可信消息模块生成所述本地计算设备的所述可信执行环境的本地证明引用的装置；以及用于由所述本地可信消息模块向所述远程可信消息模块传输用于证明所述本地计算设备的所述生成的本地证明引用的装置。

[0109] 示例46包括如示例42至45中任一项所述的主题，并且其中，所述用于交换所述密钥的装置包括：用于由所述本地可信消息模块从所述远程可信消息模块接收第一对称密钥以用于对传输至所述远程计算设备的消息进行认证加密的装置；用于由所述本地可信消息模块生成第二对称密钥以用于与所述远程计算设备进行通信的装置；以及用于将所述第二对称密钥从所述本地可信消息模块传输至所述远程可信消息模块以用于对从所述远程计算设备传输至所述本地计算设备的消息进行认证加密的装置。

[0110] 示例47包括如示例42至46中任一项所述的主题，并且其中，所述用于交换所述密钥的装置包括：用于由所述本地可信消息模块从所述远程可信消息模块接收第一公共密钥以用于对传输至所述远程计算设备的消息进行加密并对从所述远程计算设备接收到的已签名消息的签名进行验证的装置；用于由所述本地可信消息模块生成密钥对以用于与所述远程计算设备进行通信的装置，所述密钥对包括私有密钥和第二公共密钥；用于将所述第

二公共密钥从所述本地可信消息模块传输至所述远程可信消息模块以用于对传输至所述本地计算设备的消息进行加密并对从所述本地计算设备接收到的已签名消息的签名进行验证的装置。

[0111] 示例48包括如示例42至47中任一项所述的主题，并且其中，所述用于将所述传出消息安全地传输至所述远程计算设备的装置包括：用于由所述本地可信消息模块从所述消息客户端接收生成的消息的装置；用于由所述本地可信消息模块利用所述生成的私有密钥来对所述消息进行签名的装置；用于由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述消息进行加密的装置；以及用于由所述本地可信消息模块将所述已加密并签名的消息传输至所述远程可信消息模块的装置。

[0112] 示例49包括如示例42至48中任一项所述的主题，并且进一步包括：用于将所述生成的消息的所有部分合并成封装消息的装置，其中，所述用于对所述消息进行签名的装置包括用于对所述封装消息进行签名的装置；并且所述用于对所述消息进行加密的装置包括用于对所述封装消息进行加密的装置。

[0113] 示例50包括如示例42至49中任一项所述的主题，并且其中，所述用于合并所述生成的消息的所述部分的装置进一步包括用于压缩所述生成的消息的装置。

[0114] 实施例51包括如示例42至50中任一项所述的主题，并且其中，所述用于安全地接收来自所述远程计算设备的所述传入消息的装置包括：用于由所述本地可信消息模块接收来自所述远程可信消息模块的已加密并签名的消息的装置；用于由所述本地可信消息模块利用所述生成的私有密钥来对所述已加密并签名的消息进行解密的装置；用于由所述本地可信消息模块利用从所述远程可信消息模块接收到的所述第一公共密钥来对所述已加密并签名的消息的签名进行验证的装置；以及用于由所述本地可信消息模块将所述已解密并验证的消息转发至所述消息客户端的装置。

[0115] 示例52包括如示例42至51中任一项所述的主题，并且进一步包括：用于将所述已解密并验证的消息解封装成组成部分的装置；其中，所述用于转发所述已解密并验证的消息的装置包括用于转发所述组成部分的装置。

[0116] 示例53包括如示例42至52中任一项所述的主题，并且其中，所述用于对所述已解密并验证的消息进行解封装的装置进一步包括用于对所述已解密并验证的消息进行解压缩的装置。

[0117] 示例54包括如示例42至53中任一项所述的主题，并且其中，所述消息客户端包括以下各项之一：电子邮件客户端、即时消息传送客户端、文本消息传送客户端、图像消息传送客户端、视频消息传送客户端或音频消息传送客户端之一。

[0118] 示例55包括如示例42至54中任一项所述的主题，并且进一步包括：用于由所述本地可信消息模块判定所述远程计算设备是否已经启用所述远程可信消息模块的装置；以及用于由所述本地可信消息模块响应于确定所述远程可信消息模块未被启用而请求所述远程计算设备启用所述远程可信消息模块的装置。

[0119] 示例56包括如示例42至55中任一项所述的主题，并且其中，所述用于请求所述远程计算设备启用所述远程可信消息模块的装置包括用于向所述远程计算设备的用户提供用于安装可信消息模块的指令的装置。

[0120] 示例57包括如示例42至56中任一项所述的主题，并且进一步包括：用于由所述本

地可信消息模块从所述本地计算设备的联系人数据库中选择联系人的装置;用于由所述本地可信消息模块对所述选择的联系人构建消息请求在所述联系人的计算设备上启用可信消息模块的消息的装置;以及用于由所述本地可信消息模块将所述消息传输至所述选择的联系人的相应消息地址的装置。

[0121] 示例58包括如示例42至57中任一项所述的主题,并且其中,所述用于请求启用所述可信消息模块的装置包括用于:向所述选择的联系人提供用于在所述联系人的所述计算设备上安装可信消息模块的指令的装置。

[0122] 示例59包括如示例42至58中任一项所述的主题,并且进一步包括:用于由所述本地可信消息模块生成用于接收消息的私有消息接收地址的装置;以及用于由所述本地可信消息模块通知所述远程可信消息模块将针对所述本地计算设备的消息传输至所述私有消息接收地址的装置。

[0123] 示例60包括如示例42至59中任一项所述的主题,并且进一步包括:用于由所述本地可信消息模块接收定向至所述私有消息接收地址的消息的装置;以及用于由所述本地可信消息模块将所述接收的消息转发至所述消息客户端的装置。

[0124] 示例61包括如示例42至60中任一项所述的主题,并且进一步包括:用于由所述本地可信消息模块判定定向至所述私有消息接收地址的所述消息的发送方是否被授权使用所述私有消息接收地址的装置,其中,所述用于将所述接收的消息转发至所述消息客户端的装置包括:用于响应于确定了所述发送方被授权使用所述私有消息接收地址而将所述接收的消息转发至所述消息客户端的装置。

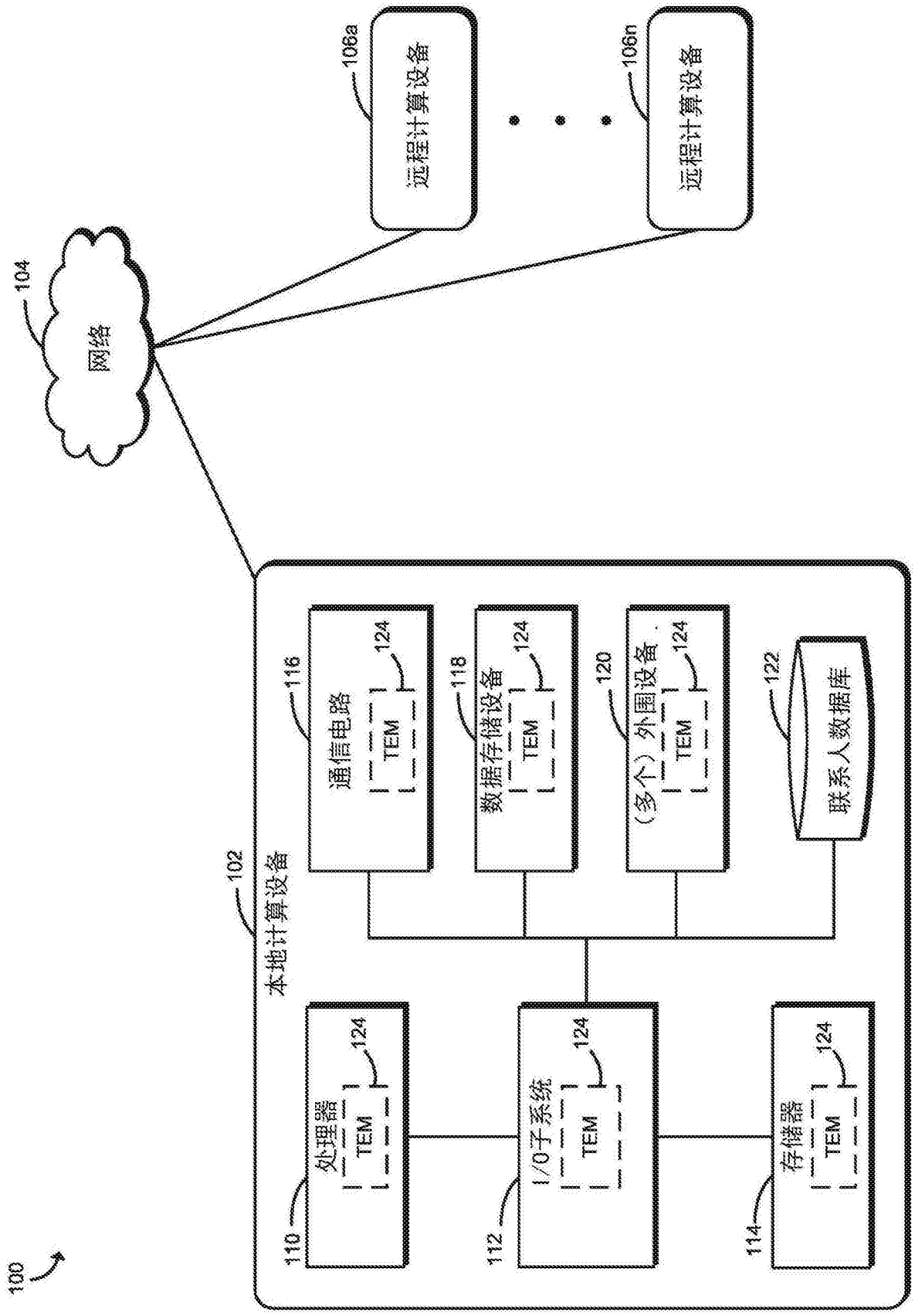

100
网络
104
远程计算设备
106a
远程计算设备
106n
本地计算设备
102
通信电路
116
数据存储设备
118
(多个)外围设备
120
联系人数据库
122
处理器
110
I/O子系统
112
存储器
114
TEM
124

图1

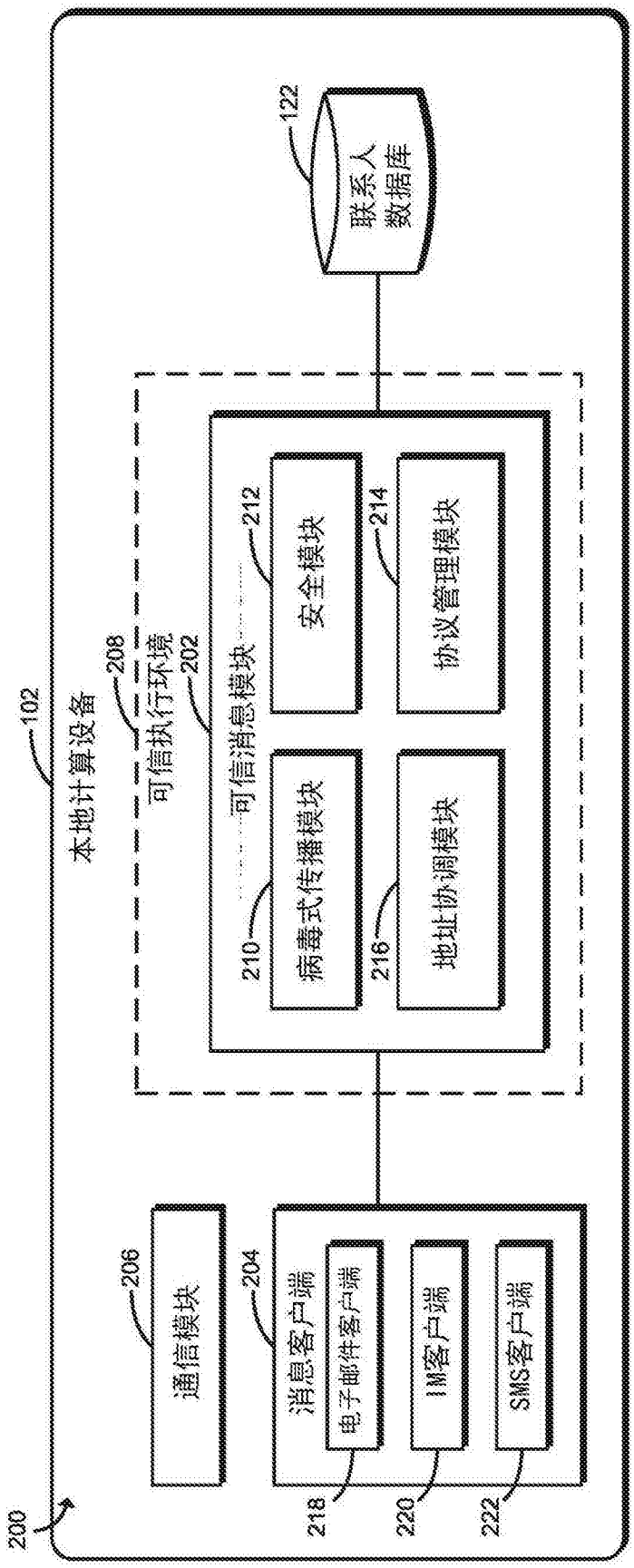

200
102
本地计算设备
208
可信执行环境
202
可信消息模块
212
安全模块
214
协议管理模块
210
病毒式传播模块
216
地址协调模块
122
联系人数据库
206
通信模块
204
消息客户端
电子邮件客户端
IM客户端
SMS客户端
218
220
222

图2

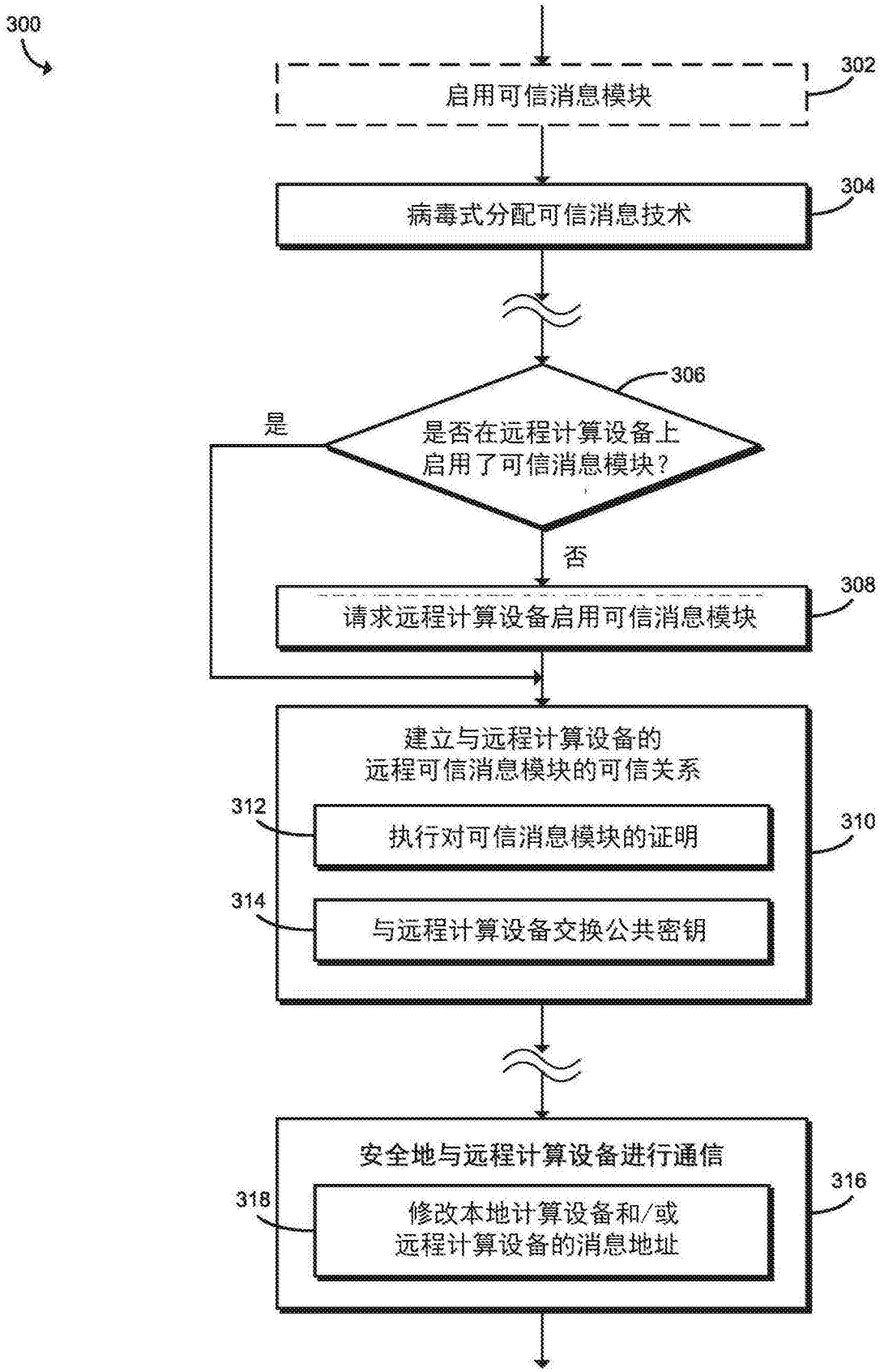

300
302
启用可信消息模块
304
病毒式分配可信消息技术
306
是否在远程计算设备上
启用了可信消息模块?
是
否
308
请求远程计算设备启用可信消息模块
建立与远程计算设备的
远程可信消息模块的可信关系
312
执行对可信消息模块的证明
314
与远程计算设备交换公共密钥
310
安全地与远程计算设备进行通信
318
修改本地计算设备和/或
远程计算设备的消息地址
316

图3

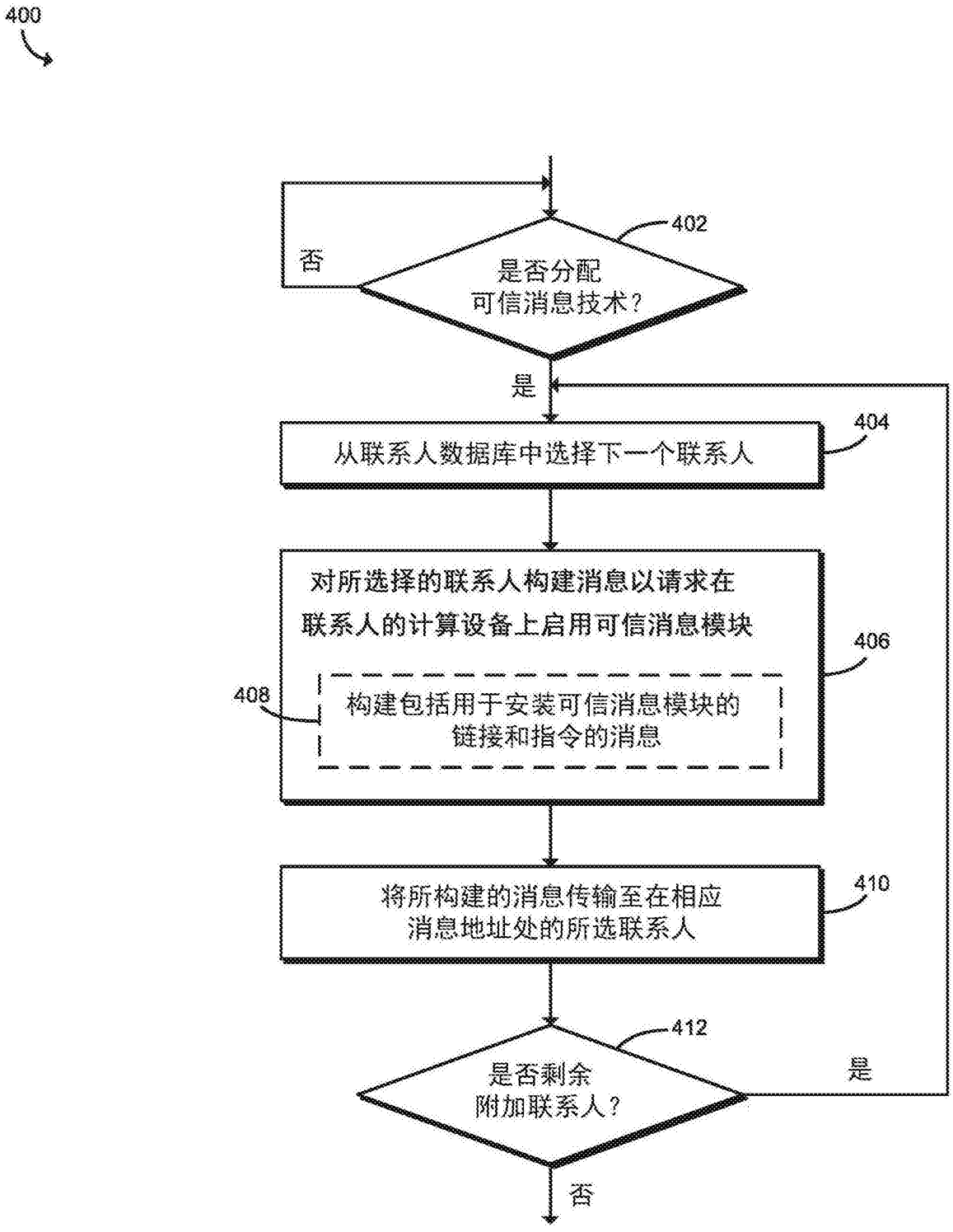

400
402
否
是否分配
可信消息技术？
是
404
从联系人数据库中选择下一个联系人
对所选择的联系人构建消息以请求在
联系人的计算设备上启用可信消息模块
406
408
构建包括用于安装可信消息模块的
链接和指令的消息
410
将所构建的消息传输至在相应
消息地址处的所选联系人
412
是否剩余
附加联系人？
是
否

图4

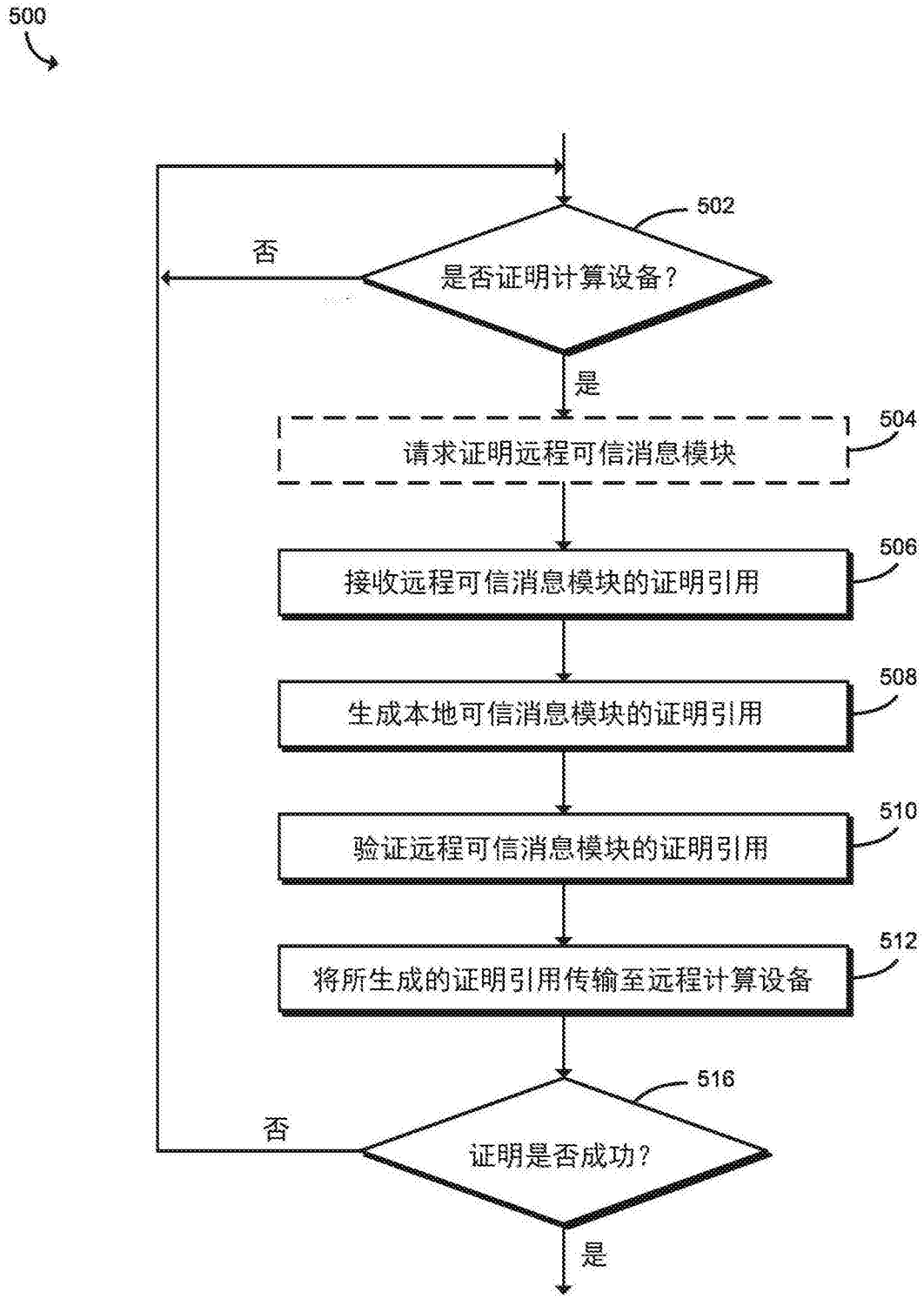

500
502
是否证明计算设备？
否
是
504
请求证明远程可信消息模块
506
接收远程可信消息模块的证明引用
508
生成本地可信消息模块的证明引用
510
验证远程可信消息模块的证明引用
512
将所生成的证明引用传输至远程计算设备
516
证明是否成功？
否
是

图5

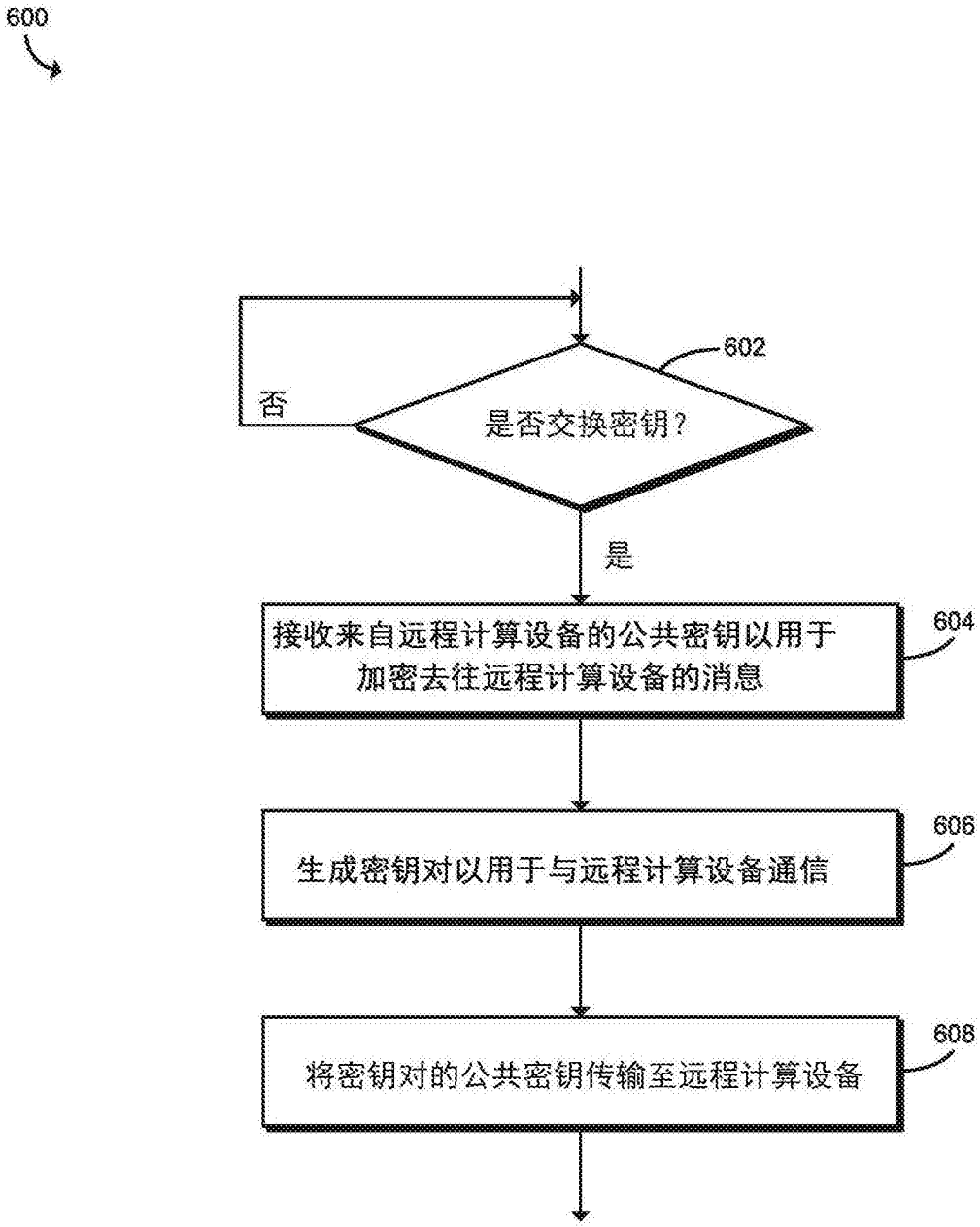

600
602
否
是否交换密钥？
是
接收来自远程计算设备的公共密钥以用于加密去往远程计算设备的消息
604
生成密钥对以用于与远程计算设备通信
606
将密钥对的公共密钥传输至远程计算设备
608

图6

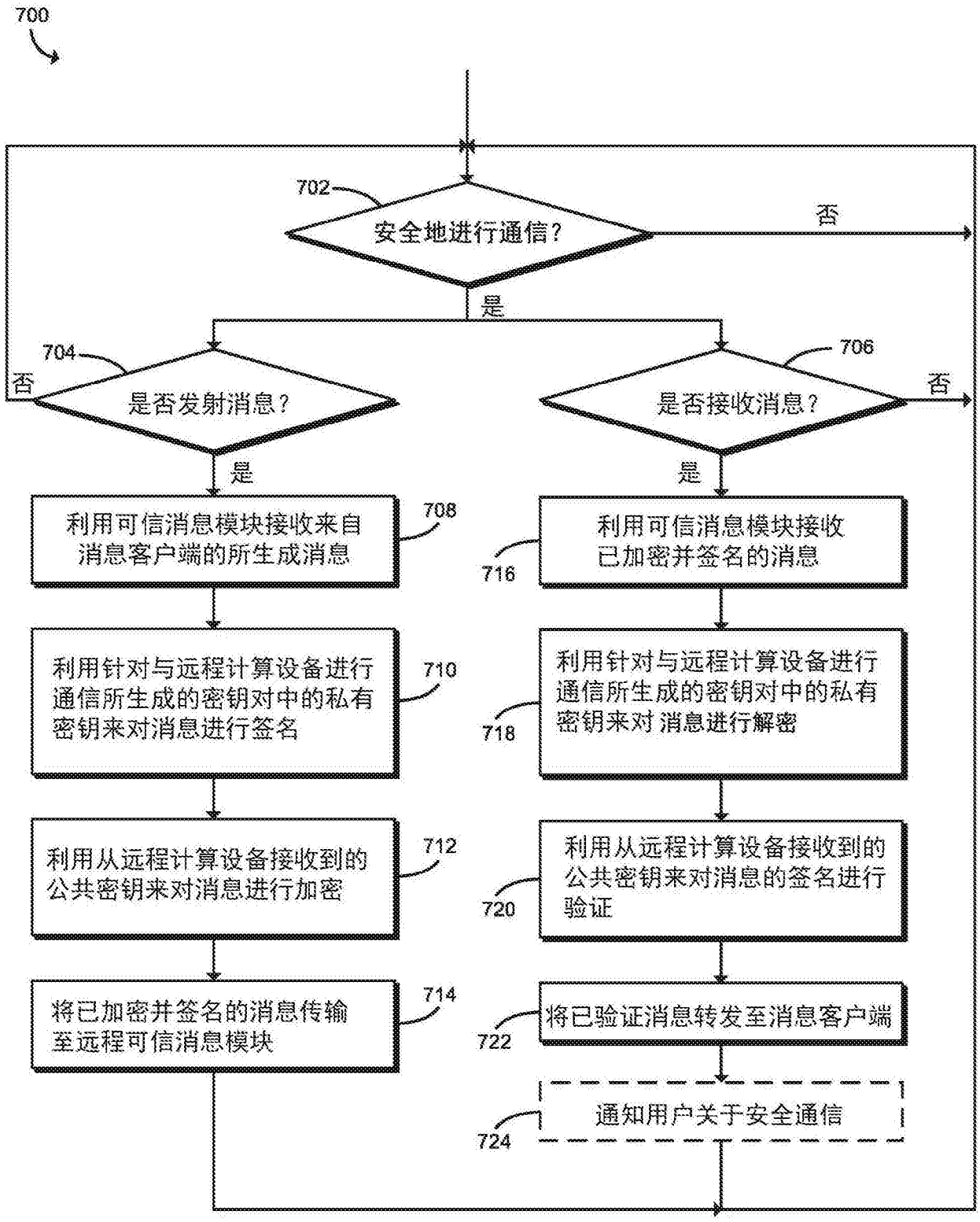

700
702
安全地进行通信？
否
是
704
否
是否发射消息？
706
是否接收消息？
否
是
是
利用可信消息模块接收来自消息客户端的所生成消息
708
利用针对与远程计算设备进行通信所生成的密钥对中的私有密钥来对消息进行签名
710
利用从远程计算设备接收到的公共密钥来对消息进行加密
712
将已加密并签名的消息传输至远程可信消息模块
714
716
利用可信消息模块接收已加密并签名的消息
718
利用针对与远程计算设备进行通信所生成的密钥对中的私有密钥来对 消息进行解密
720
利用从远程计算设备接收到的公共密钥来对消息的签名进行验证
722
将已验证消息转发至消息客户端
724
通知用户关于安全通信

图7

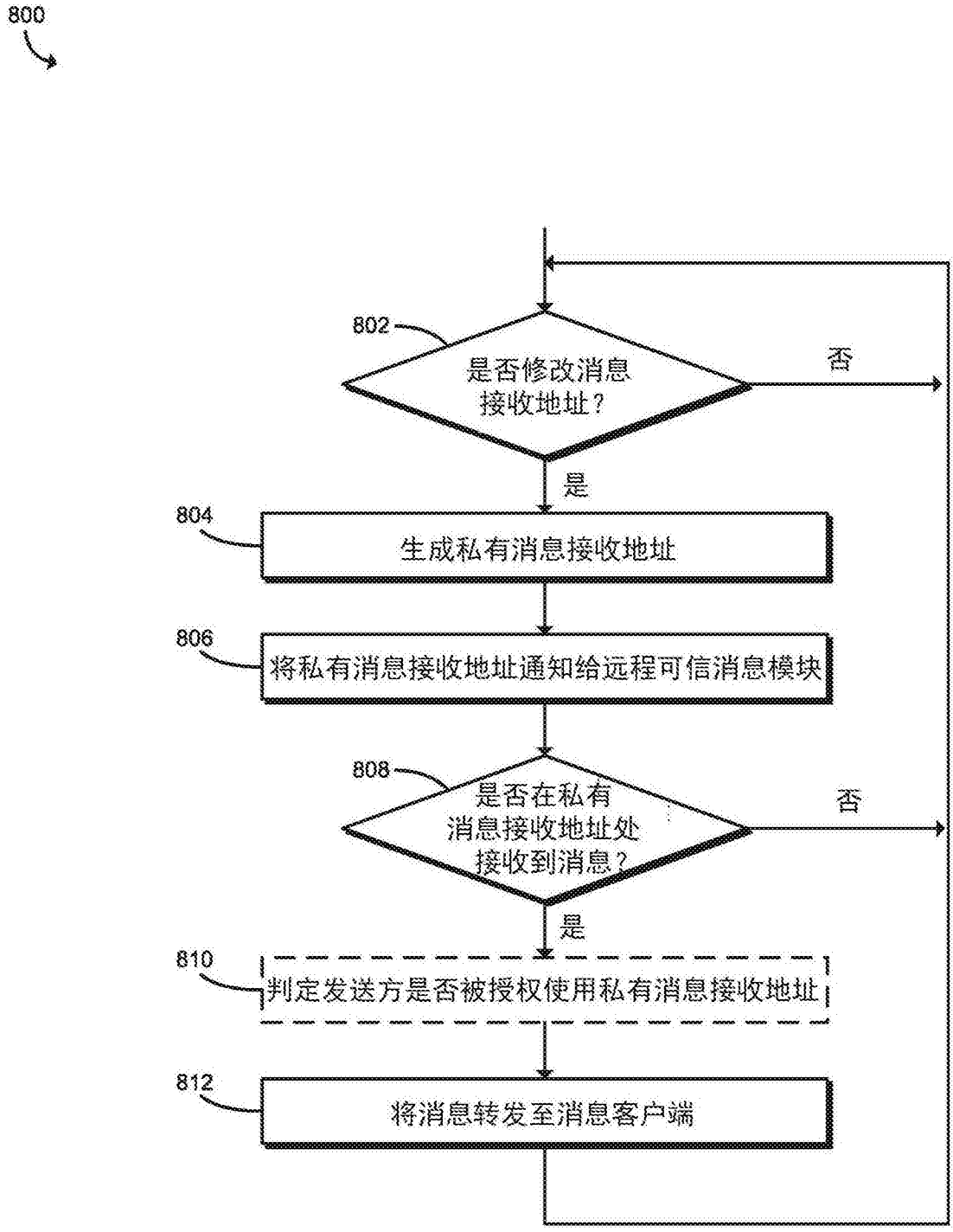

800
802
是否修改消息接收地址？
否
是
804
生成私有消息接收地址
806
将私有消息接收地址通知给远程可信消息模块
808
是否在私有消息接收地址处接收到消息？
否
是
810
判定发送方是否被授权使用私有消息接收地址
812
将消息转发至消息客户端

图8