(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1713197 B
(45)授权公告日 2013.05.29

(21)申请号 200510071412.5
(22)申请日 2005.05.13
(30)优先权数据
10/868,116 2004.06.15 US
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 C·A·米科 D·E·黑克曼
J·D·本纳龙 J·T·古德曼
M·佩纳多
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运
(51)Int.Cl.
G06F 17/60(2006.01)

(56)对比文件
CN 1379893 A,2002.11.13, 说明书摘要.

审查员 李小青

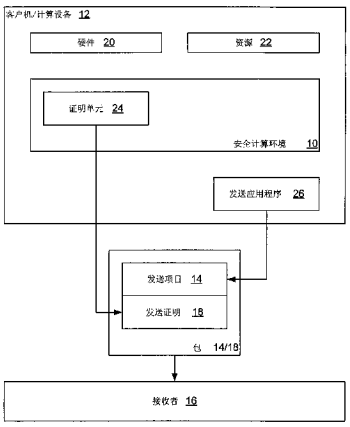
权利要求书2页 说明书10页 附图4页

(54)发明名称

通过计算机设备上可信组件验证与计算机实体的人类交互的方法

(57)摘要

一方法，描述与从计算设备的应用程序发送—发送项目到接收者有关的用户交互。该计算设备在其上具有证明单元用于证明可信赖性。该应用程序方便了用户构造发送项目，并监视预定标记，它能够用于检测实际上用户是否正花费努力来构造发送项目。证明单元认证应用程序以给予其信任，且基于用户命令应用程序发送，构造发送证明以伴随发送项目。发送证明基于受监视标记和应用程序认证，并从而描述了用户交互。所构造的发送证明与构造的发送项目被打包，且将该包发送给接收者。



CN 1713197 B

1. 一种从计算设备的应用程序发送一发送项目到一接收者的方法，所述计算设备具有一证明单元用于证明所述应用程序或发送项目的可信赖性，其特征在于，所述方法包括：

所述计算设备上的应用程序构造所述发送项目；

所述应用程序和所述证明单元之一监视预定因素并将所监视的因素信息附加到所述发送项目中，所述预定因素用来检测和收集构造所述发送项目所花费的人类努力；

所述证明单元认证所述应用程序以信任所述应用程序；

当发出将所构造的发送项目发送给所述接收者的命令时，所述应用程序和所述证明单元之一构造一发送证明来伴随所述发送项目，所述发送证明包括一个或多个所监视的因素和在所述发送项目的构造中人类所使用的资源的应用程序的认证，所述因素指示了构造所述发送项目所花费的人类努力；

所述证明单元和所述应用程序之一将所构造的发送证明与所构造的发送项目打包在一起；以及

所述证明单元和所述应用程序之一将打包的发送项目和发送证明发送给所述接收者。

2. 如权利要求 1 所述的方法，其特征在于，所述应用程序包括所述计算设备上的电子邮件应用程序，以构造要发送给所述接收者的电子邮件消息。

3. 如权利要求 1 所述的方法，其特征在于，所述应用程序包括所述计算设备上的请求应用程序，以构造要发送给所述接收者的请求。

4. 如权利要求 1 所述的方法，其特征在于，所述预定因素包括下列各项至少之一：键盘活动的最小度量的量、写字板活动的最小度量的量、鼠标活动的最小度量的量和缺少用于控制所述应用程序活动的运行脚本。

5. 如权利要求 1 所述的方法，其特征在于，所述预定因素包括下列各项至少之一：构造所述发送项目的最小构造时间和每单位时间所发送的发送项目的最大数量。

6. 如权利要求 1 所述的方法，其特征在于，其中所述证明单元通过审查附加给所述证明的数字证书来认证所述应用程序。

7. 如权利要求 1 所述的方法，其特征在于，所述计算设备包括资源，所述方法还包括所述证明单元对构造所述发送项目中所使用的所述计算设备的资源进行认证。

8. 如权利要求 7 所述的方法，其特征在于，其中所述证明单元通过审查由所述资源的每一项目提供的数字证书来认证该资源。

9. 如权利要求 1 所述的方法，其特征在于，所述方法还包括所述应用程序和所述证明单元中的一个根据所述受监视因素确定预定要求是否已满足，以及如果是则构造所述发送证明。

10. 如权利要求 1 所述的方法，其特征在于，其中所述发送证明还包括：

描述所述应用程序和相关于所述应用程序的信息的陈述；以及

描述所述发送项目和与所述发送项目有关的信息的陈述，包括与所述受监视的因素的度量的值有关的信息。

11. 如权利要求 10 所述的方法，其特征在于，所述计算设备包括硬件和资源，所述方法还包括所述证明单元认证在构造所述发送项目中所使用的所述计算设备的资源，所述方法还包括构造所述发送证明以包括描述所述资源及与这些资源有关的信息的陈述。

12. 如权利要求 1 所述的方法，其特征在于，其中将所构造的发送证明与所构造的发送

项目打包的步骤是通过将所述发送证明附加到所述发送项目、根据所述证明单元的密钥签名打包的发送项目 / 发送证明以形成数字签名、并将所述数字签名附加到所述打包的发送项目 / 发送证明来完成的。

13. 一种用于描述与从计算设备的应用程序发送发送项目到接收者有关的用户交互的方法，所述计算设备具有用于证明所述应用程序或发送项目的可信赖性的证明单元，其特征在于，所述方法包括 ：

所述计算设备上的应用程序便于用户构造所述发送项目 ；

所述应用程序和所述证明单元之一监视预定因素并将所监视的因素信息附加到所述发送项目中，所述预定因素用来检测和收集构造所述发送项目所花费的人类努力 ；

所述证明单元认证所述应用程序以信任所述应用程序 ；

当所述用户命令所述应用程序发送所构造的发送项目到所述接收者时，所述应用程序和所述证明单元之一构造一发送证明以伴随所述发送项目，所述发送证明包括一个或多个所监视的因素和在所述发送项目的构造中人类所使用的资源的所述应用程序的认证，所述因素指示了构造所述发送项目所花费的人类努力，其中所监视的因素包括所度量的与至少一个硬件设备的人类交互 ；

所述证明单元和所述应用程序之一将所构造的发送证明与所构造的发送项目打包在一起 ；以及

所述证明单元和所述应用程序之一将所打包的发送项目和发送证明发送给所述接收者。

通过计算机设备上可信组件验证与计算机实体的人类交互的方法

技术领域

[0001] 本发明涉及一种结构和方法，用于向计算机实体验证，结合计算设备进行的计算机请求是由人类发起的而不是由计算机应用程序等发起的。更具体地，本发明涉及这样一种结构和方法，由此通过计算设备上运行的可信组件执行验证。

背景技术

[0002] 存在人类交互证据以向计算机实体证明，来自计算设备的对该实体的请求是由在该计算设备处的人类发起的，而不是由在该计算设备上运行的应用程序发起的。因而，这样一个人类交互证据可以由例如网站使用来确认对站点 ID 的请求来自为可能合法的目的试图获得单一站点 ID 的人，且这样的请求不是来自为可能非法或至少不受欢迎的目的试图获得多个站点 ID 的计算机应用程序。如可意识到的，在后者情况下，这样的多个站点 ID 可能被例如希望躲在这样的多个站点 ID 后面以便避免诚实地标识自己的恶意实体使用。

[0003] 这样一个人类交互证据还可被例如消息接收者使用来确认消息的发送者是为可能受欢迎的目的试图向该接收者发送个人消息的人，且这样的消息不是来自为可能不受欢迎的目的试图发送多个非个人的成批消息的计算机应用程序。如可意识到的，在后者情况下，这样的多个批量消息可以例如采用广告或‘垃圾邮件’的形式，来自与该接收者没有个人关系的恶意实体。

[0004] 人类交互证据还可被例如在线广告商使用，它向在线中介支付介绍费，每当由中介提供的链路被用户选择时。这里，证据确认消息来自希望经由链路访问广告商的人类选择用户，且这样的消息不是来自试图从中介或其代理发送多个非个人的批量消息给广告商的计算机应用程序。如可意识到的，在后者情况下，这样的多个批量消息例如可只被发送来生成介绍费，即使没有涉及最终用户，而且有时称之为‘欺诈点击 (fraudulent click-through)’。如也可意识到的，这样的欺诈点击可发生在广告环境中和在中介有动机生成这种消息的其 它环境中。

[0005] 更普遍地，要理解使用人类交互证据来防止不想要的批量发送消息、在广告环境等中防止欺诈点击、在在线拍卖网站上防止掠夺性砍价、在线购买的人类证据、帐户建立的人类证据等。然后，这样的人类交互证据可在请求或消息 (下文为‘发送项目 (send item)’) 的接收者希望确保该发送项目是由在计算设备处执行人类类型动作的人类而不只是由执行编程化动作的计算设备发起的任何环境下使用。

[0006] 每个这样的人类交互证据基本上设计成要求发送上述发送项目的人类多少要花费些主动努力，其中所说的努力是具有计算设备可能无法完成的性质的动作。在人类交互证据的一个通用版本中，例如，预想接收者发送给预想发送者一个‘质询 (challenge)’，它包括可能容易地用一个词语诸如狗、球、铅笔等来描述的物品的图片，且发送者必须与该发送项目一起发送一个词语。有可能的是，如果发送者是人类，则这样的发送者能够容易地识别出质询中的图片化物品并提供该词语。也有可能的是，如果发送者不是人类而是计算设

备，则这样的发送者不能轻易地识别图片化物品并提供该词语。在人类交互证据的另一个通用版本中，预想接收者发送给预想发送者一质询，包括不希望根据可能由计算设备执行的光学字符识别协议方便识别的词语的图片，但对人而言应易于识别，且再一次发送者必须与该发送项目一起发送该词语。

[0007] 无论如何，未能与发送项目一起提供词语可能例如引起预想接收者根据发送者不是发送受欢迎发送项目的人的假设来忽略此消息。由于识别图片或词语和提供这一个词语的努力不能够轻易地由计算设备完成，因此人类交互证据在极大程度上确定请求或消息的发送者是人。

[0008] 而且，即使要识别的努力不知何故由计算设备完成了，或者恶意实体可雇用人力来完成识别，该努力在计算设备或者作为发送者的劳动力雇员上强加了开销，无论按照货币价值、容量、时间还是其它方面。例如，向一百万个接收者发送电子邮件消息的计算设备，如果对一百万条消息不要求人类交互证据，则根据当今技术可能相对很容易做到。但是，且值得注意地，如果对一百万条消息要求唯一的人类交互证据，则同样的向一百万个接收者发送电子邮件消息的计算设备必须花费巨大的努力。那么，如可意识到的，要求计算设备或人力对许多发送项目的每一个进行人类交互证据可迅速成为严峻的障碍，尤其在计算设备或劳动力雇员试图发送成百、成千或者甚至成百万的这样的发送项目的 情况下。

[0009] 然后，总结一下，人类交互证据防止了不想要的发送项目，诸如那些可由计算设备批量发送的发送项目，因为人类交互证据要求计算设备完成计算设备实际上不能完成的动作，否则就要求计算设备或人力在每个发送项目基础上完成该动作并因此花费巨大努力。但是，人类交互证据注定要受到损害，因为这样的证据要求人类为满足这样的证据而花费主动努力，而不计算人类在发送一个项目的自然过程中可能花费的被动努力。提出另一种方法，当前的人类交互证据没有认识到人类在发送一个项目中花费计算机不会同样花费的被动或自然努力，诸如例如在键盘上打字、通过鼠标设备移动光标等，以及通过检测这种被动努力的花费，人类交互证据实际上不需要人类以‘跳过环(jumpingthrought a hoop)’方式花费主动或特定的努力。

[0010] 那么，存在对一种人类交互证据(HIP)的需求，它实质上不要求人类花费主动努力，而是人类只花费被检测的自然努力。具体而言，存在对一种结构和方法的需求，它实现这样一种人类交互证据并以可信的方式向接收者验证这种检测到的自然努力，因此可以向接收者保证所检测到的恶意实体实际上发生了并且不是由企图欺骗接收者的恶意实体设计的。此外，存在对于这样一种结构和方法的需求，通过它发送者的计算设备上的可信组件完成这样的验证。

[0011] 发明概述

[0012] 上述需求至少部分由本发明满足，本发明提供了一方法，描述与从计算设备的应用程序向接收者发送发送项目结合的用户交互。计算设备在其上具有证明单元用于证明可信赖性。在该方法中，计算设备上的应用程序促进用户构造发送项目，且应用程序和证明单元之一监视可用来检测用户实际上是否正花费努力构造发送项目的预定标记。

[0013] 证明单元认证应用程序以给予其信任，且应用程序和证明单元之一在用户命令应用程序发送所构造的发送项目给接收者时，构造发送证明以伴随发送项目。发送证明基于受监视标记和对应用程序的认证，并从而描述了用户交互。证明单元和应用程序之一打包

所构造的发送证明与所构造的发送项目，且证明单元和应用程序之一将打包的发送项目和发送证明发送给接收者。

附图说明

[0014] 以上概述以及以下本发明实施例的详细描述将在与附图结合阅读时得到 更好的理解。为了说明本发明，附图中示出了目前较佳的实施例。但是，如应该理解的，本发明不限于所示的精确方案与手段。在附图中：

[0015] 图 1 是表示通用计算机系统的方框图，其中可结合本发明的各方面和 / 或其部分；

[0016] 图 2 是依照本发明的一个实施例示出具有发送应用程序和证明单元的、发送—发送项目和—发送证明给接收者的计算设备；

[0017] 图 3 和 4 是依照本发明的一个实施例示出在图 2 的计算设备（图 3）和接收者（图 4）处执行的关键步骤的流程图。

[0018] 详细说明

[0019] 计算机环境

[0020] 图 1 及以下讨论旨在提供本发明和 / 或其部分可在其中实现的合适计算环境的简要描述。尽管不是必需，但本发明在由诸如客户机工作站或服务器的计算机执行的诸如程序模块的计算机可执行指令的通用上下文环境中描述。通常，程序模块包括例程、程序、对象、组件、数据结构等，执行特定任务或实现特定抽象数据类型。而且，应该理解本发明和 / 或其部分可用其它计算机系统配置实施，包括手持设备、多处理器系统、基于微处理器和可编程消费电子产品、网络 PC、小型机、主机计算机等。本发明还可在分布式计算环境中实施，其中任务由通过通信网络连接的远程处理设备完成。在分布式计算环境中，程序模块可位于本地和远程存储器存储设备。

[0021] 如图 1 所示，示例性通用计算设备包括常规的个人计算机 120 等，包括处理单元 121、系统存储器 122 和系统总线 123（将包括系统存储器在内的各种系统组件耦合到处理单元 121）。系统总线 123 是任意若干类型的总线结构，包括存储器总线或存储器控制器、外围总线和使用任何各种总线体系结构的局部总线。系统存储器包括只读存储器 (ROM)124 和随机存取存储器 (RAM)125。基本输入 / 输出系统 126(BIOS)，包含诸如在起动时，帮助在个人计算机 120 内在元件之间传送信息的基本例程，BIOS 被存储在 ROM124 中。

[0022] 个人计算机 120 还可包括用于读写硬盘（未示出）的硬盘驱动器 127，用于读或写可移动磁盘 129 的磁盘驱动器 128，和用于读写可移动光盘 131 如 CD-ROM 或其它光介质的光盘驱动器 130。硬盘驱动器 127、磁盘驱动器 128 和光盘驱动器 130 分别通过硬盘驱动器接口 132、磁盘驱动器接口 133 和光盘驱 动器接口 134 连接到系统总线 123。驱动器及其相关联的计算机可读介质为个人计算机 120 提供计算机可读指令、数据结构、程序模块和其它数据的非易失性存储。

[0023] 尽管这里描述的示例性环境使用硬盘、可移动磁盘 129 和可移动光盘 131，但应当意识到，存储计算机能存取的数据的其它类型计算机可读介质也可在示例性操作环境中使用。这样的其它类型介质包括磁盒、闪存卡、数据视频盘、Bernoulli 盒、随机存取存储器 (RAM)、只读存储器 (ROM) 等等。

[0024] 许多程序模块可存储在硬盘、磁盘 129、光盘 131、ROM124 或 RAM125 上，包括操作系统 135、一或多个应用程序 136、其它程序模块 137 和程序数据 138。用户可通过输入设备诸如键盘 140 和指点设备 142 输入命令和信息到个人计算机 120 中。其它输入设备（未示出）可包括话筒、游戏杆、游戏垫、卫星天线等等。这些和其它输入设备常常通过耦合到系统总线的串行口端口 146 连接到处理单元 121，但也可通过其它接口如并行端口、游戏端口或通用串行总线 (USB) 连接。监示器 147 或其它类型的显示设备也通过接口如视频适配器 148 连接到系统总线 123。除监示器 147 之外，个人计算机一般包括其它外围输出设备（未示出），诸如扬声器和打印机。图 1 的示例性系统还包括主机适配器 155、小型计算机系统接口 (SCSI) 总线 156 和连接到 SCSI 总线 156 的外部存储设备 163。

[0025] 个人计算机 120 可在使用到一个或多个远程计算机如远程计算机 149 的逻辑连接的网络化环境中使用。远程计算机 149 可以是另一个个人计算机、服务器、路由器、网络 PC、对等设备或其它公共网络节点，并且一般包括上面相对于个人计算机 120 所述的许多或全部元件，尽管在图 1 中只示出了存储器存储设备 150。图 1 所示的逻辑连接包括局域网 (LAN)151 和广域网 (WAN)152。这样的网络环境在办公室、企业级计算机网络、企业内部互联网和因特网中很常见。

[0026] 当在 LAN 网络环境中使用时，个人计算机 120 通过网络接口或适配器 153 连接到 LAN151。当在 WAN 网络环境中使用时，个人计算机 120 一般包括用于在广域网 152 如因特网上建立通信的调制解调器 154 或其它装置。调制解调器 154，可以是内置或外置的，通过串行端口 146 连接到系统总线 123。在网络化环境中，相对个人计算机 120 所述的程序模块或其部分可存储在远程存储器存储设备中。将意识到，所示的网络连接是示例性的并且可以使用在计算机之间 建立通信链路的其它方法。

[0027] 通过检测被动努力验证人类交互

[0028] 在本发明中，提供一种方法和系统来实现人类交互证据 (HumanInteractive Proof)，它验证人类涉及了计算事务，通过该方法和系统，这个人要发送项目给接收者。在该证据中，并且一般地所发送的项目伴随着一个发送证明，它陈述实际检测的与所发送的项目有关的足够人类努力的效果，并且因此计算机不是简单地基于在每发送项目基础上不要求任何有效的人类努力的程序或应用程序来发送项目。检测到的足够的人类努力例如可包括键击、鼠标点击、键击或鼠标点击的最小数量、最小撰写时间、接收者的最大数量的选择、每单位时间交付的发送项目的最大数量等等。在本发明中，被动地检测人类交互，因此人类不必结合发送证明发挥任何主动努力。因而，人类交互是基于人在构造和发送—发送项目给其接收者的过程中通常承担的活动来检测的。

[0029] 为给予发送证明信任，现在转到图 2，这样的发送证明 18 是由或者代表在发送项目 14 的发送者的计算设备 12 上运行的安全计算环境 10 撰写的，其中安全计算环境 10 是要由接收者 16 信任的。如可意识到的，发送项目 14 是由或者结合计算设备 12 构造的，诸如例如在运行于计算设备 12 的发送应用程序 26 的帮助下，并且发送证明 18 也是在计算设备 12 上撰写的。安全计算环境 10 配置为在可信的基础上提供发送证明 18 给接收者 16 以确认，关于相应发送项目 14 的构造，检测到足够的人类努力，再次在被动基础上而不要求人类的任何主动卷入。在不同实施例中，发送项目 14 包括发送证明 18 作为附属物等，或者发送证明 18 与发送项目 14 分开但链接到它，可能通过指针或其它引用。

[0030] 发送者的计算设备 12 可以是不脱离本发明精神和范围的任何适当的计算设备。例如，计算设备可以是个人计算机、便携式通信设备、无线通信设备等等。这样的计算设备 12 适当地通过适当的通信链路耦合到接收者 16。这样的链路可以是直接连接或者可以是网络连接，诸如使用适当通信协议的网络内部或之间的连接。

[0031] 接收者 16 通常是运行于远离计算设备 12 或者在其本地的服务器、计算机或其它计算设备上的应用程序。这样的接收者 16 可提供服务给计算设备 12 处的发送者，基于来自它的请求，在本例中以发送项目 14 的形式。因而，发送项目 14 可以是对一段内容的请求、对用户 ID 的请求、对网络资源的请求等等。接收者 16 另外可接收在那里的用户的消息，在本例中再次以发送项目 14 的形 式。因而，发送项目 14 也可以是例如以邮件项目形式的网络消息。然后，应当意识到，发送项目 14 适当地以相应的接收者 16 为目标。因此，这样的发送项目 14 和相应的接收者 16 可以是不脱离本发明的精神和范围的任何适当的发送项目 14 和接收者 16。

[0032] 在发送项目 14 的发送者的计算设备 12 上运行的安全计算环境 10 是如上所述的由接收者 16 信任的安全计算环境。因而，安全计算环境 10 应当能够向接收者 16 证明这样的信任，诸如例如通过能够提供密钥、数字签名、数字证书等等。通常，这样的数字证书包括引回到根信任当局的证书链，并且接收者 16 接受数字证书并基于它准予信任，如果接收者 16 识别和承兑这样的证书的根信任当局。

[0033] 如可意识到的，在发送者的计算设备 12 上运行的安全计算环境 10 应当免于由在其计算设备 12 上运行的其它实体的控制，或者免于由来自其它计算设备或人类形式的控制。因而，安全计算环境 10 应当不能被强制在不保证发送证明 18 的时候发出这样的发送证明，诸如例如如果一个邪恶实体想要在没有适当的人类交互的情况下发出发送项目 14 的时候。

[0034] 这样的安全计算环境 10 可以是不脱离本发明精神和范围的、服从在此所述的约束过程的任何适当的安全计算环境。例如，安全计算环境 10 可以是在计算设备 12 上的操作系统的可信部分，其中这样的操作系统的可信部分免于不适当的外部影响。安全计算环境 10 或者可自己检测与发送项目 14 有关的足够的人类努力，或者可在运行于其上的某应用程序和可能有关的硬件中给予信任以如此检测，并且同样或者可自己在适当的时候构造发送项目 14 的发送证明 18，或者可在运行于其上的某应用程序中给予信任以如此构造。在本发明的一个实施例中，安全计算环境 10 实际上包括证明单元 24 作为在其上运行的应用程序和 / 或在其中运行的硬件以检测上述足够的人类努力和构造上述发送证明 18。

[0035] 证明单元 24 可以是不脱离本发明的精神和范围的任何适当的硬件和 / 或软件。例如，证明单元 24 可以被建立为在安全计算环境 10 的可信区域中运行的软件，或者可以是在计算设备 12 上被设计为执行在此所述的证明功能的一部分硬件。在任一情况下，这样的证明单元 24 被保护不受在计算设备上运行的任何其它软件或硬件监视或影响，尤其是被保护不受诸如由企图破坏证明单元 24 的功能的邪恶实体使用的攻击。证明单元 24 于是应当被设计为防篡改，并 且应当能够以数字方式签名、验证签名、加密、解密等等。这样的证明单元 24 至少应当对于熟练技术人员是显然的并且因此在此不必更详细地描述。

[0036] 注意，安全计算环境 10 和 / 或其证明单元 24 在检测是否有可能已经花费了足够的人类努力时必须接受从计算设备 12 上的硬件 20 得到的输入、所述硬件是人类在构造发

送项目 14 的过程中将使用的。例如，这样的硬件 20 可包括触摸屏、键盘、光标控制设备如鼠标等等。另外，安全计算环境 10/ 证明单元 24（在下文中，‘证明单元 24’）可指计算设备 12 的其它资源 22，诸如时钟、存储器、控制器等等。然后，每个这样的一部分硬件 20 和每个这样的资源 22 可变成一种途径，邪恶实体可能通过它企图不适当地破坏对与发送项目 14 有关的足够的人类努力的花费的检测。因此，在本发明的一个实施例中，每个这样的一部分硬件 20 和每个这样的资源 22 被构造为由证明单元 24 信任，并且还能够向证明单元 24 证明这样的信任，诸如例如通过能够提供密钥、数字签名、数字证书等等。再次，这样一个数字证书一般包括引回到根信任当局的证书链，并且安全计算环境 10 接受数字证书并且基于它准予信任，如果这样的证明单元 24 识别并且承兑这样的证书的根信任当局。

[0037] 发送证明 18 本身可采用不脱离本发明的精神和范围的任何适当形式。例如，发送证明 18 可基于某种形式可扩展标记语言 (XML) 构造为数字文档并基于私钥以数字方式签名，并且按照可从上述安全计算环境 10 的数字证书得到的相应的公钥是可验证的。因而，这样的发送证明 18 可包括这样的数字证书，并且也可包含某种肯定陈述，它证明这样的事实 :检测到足够的人类努力花费在构造相应发送项目 14 的过程中。另外，它可以是这样一种情况，即发送证明 18 包括与这样检测到的所花费的人类努力有关的细节，诸如例如键击数、用于构造发送项目 14 的时间量、接收者 16 的数量等、在预先预定义时段内发送的发送项目 14 的数量，和 / 或与所使用的硬件 20 和 / 或资源 22 有关的细节。如可意识到的，有了这样的细节，接收者 16 可在决定是否承兑发送项目 14 的过程中执行附加的过滤。

[0038] 然后概括一下，在本发明中，发送—发送项目 14 给接收者 16 的发送用户使用计算设备 12，它具有硬件 20，包括某种输入设备诸如键盘、鼠标等 ；资源 22，包括存储器等 ；应用程序 26，用于构造发送项目 14 ；和受信托的证明单元 24，在不会受用户影响和能证明发送项目 14 的安全计算环境 10 中运行。接收者 16 在接收发送项目 14 并伴随发送证明 18 时，只有当伴随该发送项目 14 的发送证明 18 对于这样的接收者 16 是可接受的时候才承兑该发送项目 14。现在转到图 3，示出由和 / 或结合上述组件使用的方法。

[0039] 首先，预期在计算设备 12 处的用户通过发送应用程序 26 构造发送项目 14（步骤 301）。当然，如果发送项目 14 是消息，则应用程序 26 是消息 - 发送应用程序诸如电子邮件应用程序，而如果发送项目 14 是请求，则应用程序 26 是能够撰写请求的应用程序，诸如例如基于从接收者 16 接收的代码的计算机浏览器。

[0040] 结合在步骤 301 构造发送项目 14，应用程序 26 和证明单元 24 之一监视某些预定标记，它们可以用于检测用户实际上正在花费努力构造发送项目 14（步骤 303），以及应用程序 26 不是自己以没有实际用户卷入的自动化过程方式在构造发送项目 14。这样的标记可以是不脱离本发明精神和范围的任何标记。例如，应用程序 26 或者证明单元 24 可监视实际键盘活动和 / 或鼠标活动，用于构造发送项目 14 的最小构造时间、每单位时间发送的发送项目的最大数量、用于控制应用程序 26 活动的运行脚本的缺少等等。

[0041] 明显地，在步骤 301 已经构造发送项目 14 之前或之后，证明单元 24 认证应用程序 26（步骤 305）以给予它信任。由证明单元 24 对这类应用程序 26 的这类认证例如可发生在应用程序 26 在计算设备 12 上被实例化的时候，在应用程序 26 由用户调用以构造发送项目 14 的时候，或者在发送项目 14 被构造和被发送到接收者 16 的时候。由证明单元 24 对应用程序 26 的这类认证可包括不脱离本发明精神和范围的任何适当的认证。例如，这类认

证可包括应用程序 26 为证明单元 24 提供数字证书，并且可能提供其它可使用的文档以及可能提供关于在其内应用程序 26 正在运行的环境的信息。基于这类信息证明单元 24 本身确保可以信任应用程序 26 正确地运行，例如通过验证数字证书和保证应用程序 26 正在预期的环境中基于操作的文档在运行。

[0042] 注意，尽管证明单元 24 可执行步骤 303 的监视，但应意识到，应用程序 26 本身更可能执行这样的监视。注意，这么做在应用程序 26 监视自己的范围内更简单，并且也因为证明单元 24 不是很了解应用程序 26 及其接口。无论如何，一旦证明单元 24 在步骤 305 信任应用程序 26，这样的信任就应当扩展到应用程序 26 在步骤 303 监视自己的能力。

[0043] 连同在步骤 305 认证应用程序 26 以给予其信任，证明单元 24 也可认证至少某些用于或者预期用于构造发送项目 14 的硬件 20 和 / 或资源 22（步骤 307）。 再次，由证明单元 24 对这类硬件 20 和 / 或资源 22 的这类认证例如可发生在应用程序 26 在计算设备 12 上实例化的时候，在应用程序 26 由用户调用以构造发送项目 14 的时候，或者在发送项目 14 被构造并且要被发送到接收者 16 的时候。与以前一样，这类认证可包括不脱离本发明精神和范围的任何适当的认证。例如，并且再次，这类认证可包括硬件 20 和 / 或资源 22 的若干部分的每一个为证明单元 24 提供数字证书，而且可能提供其它文档和环境信息，并且基于这类信息，证明单元 24 向自己确保例如可以信任键盘正确地操作，可以信任存储器正确地操作等等。

[0044] 无论如何，假定用户实际上已经在步骤 303 构造了发送项目，这样的用户随后命令应用程序 26 实际发送所构造的发送项目 14 给接收者 16（步骤 309）。在这么做的时候，证明单元 24 确定所有有关要求是否已经满足，基于步骤 303 所监视的标记和步骤 305 和 307 的认证（步骤 311），并且如果这样，则证明单元 24 和 / 或应用程序 26 构造发送证明 18 以伴随这样的发送项目 14（步骤 313）。之后，证明单元 24 和 / 或应用程序 26 打包所构造的发送证明 18 与所构造的发送项目 14（步骤 315），并且应用程序 26 和 / 或证明单元 24 实际上发送打包的发送项目 14 和发送证明 18 给接收者 16（步骤 317）。

[0045] 证明单元 24 可在步骤 311 以不脱离本发明精神和范围的任何适当方式确定是否已经满足所有有关要求。例如，证明单元可要求在步骤 305 和 307 的所有认证成功，并且还要求步骤 303 监视的标记满足某些预定的要求。这样的要求例如可以由证明单元 24 或接收者 16 提出。在后者的情况下，可以是接收者在某个先前的时间交付这样的要求给证明单元 24。注意，在执行步骤 311 时，证明单元可实际执行整个确定的最少部分或者根本不执行，并且将这类确定的剩余部分留给接收者 16。在这样的情况下，证明单元 24 在步骤 313 构造发送证明 18 以包括接收者 16 进行确定的剩余部分所必需的所有信息。

[0046] 证明单元 24 和 / 或应用程序 26 可在步骤 313 以不脱离本发明精神和范围的任何适当方式构造发送证明 18。例如，在本发明的实施例中，所构造的发送证明 18 包括来自证明单元 24 的陈述描述应用程序 26，并且可能包括所使用的硬件 20 和 / 或资源 22，并且还可能包括与这样的应用程序 26、硬件 20 和 / 或资源 22 诸如例如其环境有关的相关信息。如可意识到的，这类相关信息可由接收者 16 在决定是否接受和承兑发送证明 18 时和 / 或在决定是否接受和处理发送项目 14 时使用。注意，所构造的发送证明 18 也可包括来自证明单元 24 的陈述，它关于上述应用程序 26、硬件 20 和 / 或资源 22 确实是可信赖性的，不认为这样的陈述是绝对必须的，尤其是因为这样一个陈述隐含着这样的事实，即证明单元 24

选择发出描述应用程序 26 的陈述。

[0047] 明显地，所构造的发送证明 18 还包括一个陈述，描述发送项目 14，并且还包括与发送项目 14 有关的相关信息。注意，这样的陈述可来自证明单元 24 或应用程序 26。在后者的情况下，来自证明单元 24 描述应用程序 26 的的陈述至少隐含地说明可以信任发出描述发送项目 14 的陈述的应用程序 26。这里，在来自证明单元 24 或应用程序 26 的陈述中的、与发送项目 14 有关的相关信息有可能包括所监视的数据诸如与用户构造发送项目 14 有关的键盘敲击数量和 / 或鼠标点击数量、构造的时间长度、接收者 16 的数量等等。如可意识到的，并且再次，这类相关信息可由接收者 16 在决定是否接受并承兑发送证明 18 时和 / 或在决定是否接受并处理发送项目 14 时使用。再次注意，尽管所构造的发送证明 18 还可包括关于发送项目 14 确实是可信赖性的陈述，但不认为这样的陈述是绝对必须的，尤其是因为这样一个陈述隐含着这样的事实，即证明单元 24 或者应用程序 26 选择发出描述发送项目 14 的陈述。

[0048] 证明单元 24 和 / 或应用程序 26 可在步骤 315 以不脱离本发明精神和范围的任何适当方式将所构造的发送证明 18 与所构造的发送项目 14 的打包在一起。例如，在本发明的一个实施例中，发送证明 18 被添加到发送项目 14，并且组合的发送项目 14/ 发送证明 18 基于证明单元 24 的密钥被签名，以形成添加到组合的发送项目 14/ 发送证明 18 的数字签名。如已知的，这样一个数字签名可包括或者引用引回到假定接收者 16 已知并信任的根当局的证书链。

[0049] 应用程序 26 和 / 或证明单元 24 可在步骤 317 以不脱离本发明精神和范围的任何适当方式发送打包的发送项目 14 和发送证明 18 给接收者 16。例如，在本发明的一个实施例中，证明单元 24/ 应用程序 26 的计算设备 12 通过网络如在内部网络或网络之间耦合到接收者 16，在这种情况下包 14/18 可通过一或多个网络包按照相互可接受的网络通信协议来发送。

[0050] 注意，尽管此前按照执行各种动作的证明单元 24 来描述，但可以是这样的情况，即证明单元 24 只是证明并且作出关于安全计算环境 10 的陈述，并且安全计算环境 10 执行一些或全部这类动作。在这种情况下，发送证明 18 可包括描述和证明安全计算环境 10 的陈述。

[0051] 现在转到图 4，在接收具有发送项目 14 和发送证明 18 的包 14/18 时（步 骤 401），接收者 16 验证包括在其中的每个签名（步骤 403），包括基于证明单元 24 并被添加到组合的发送项目 14/ 发送证明 18 的任何签名。之后，接收者 16 检查来自证明单元 24 的、在来自在包 14/18 的发送证明 18 中阐述的陈述（步骤 405）。特别地，接收者 16 决定是否承兑发送项目，尤其是基于在发送证明 18 中阐述的描述应用程序 26 的陈述和在发送证明 18 中阐述的描述发送项目 14 的陈述。

[0052] 在本发明的一个实施例中，在发送证明 18 中阐述的这类陈述在步骤 405 中被检查，鉴于由或者代表接收者 16 阐述的预定的策略。这样的预定策略可以是不脱离本发明精神和范围的任何适当策略。例如，这类策略可阐述所述应用程序 26 必须是特定类型或版本的，或者这样描述的应用程序 26 不是特定类型或版本的。同样，这类策略可指定一个在其中应用程序 26 正在运行的特定环境，在这样的环境中不存在某一个元素，等等。

[0053] 同样，关于发送项目 14 本身，策略例如可阐述这样的发送项目 14 的特定格式，特

定编码，关于这样的发送项目的内容的限制，关于发送项目 14 的接收者的数量的限制，应当在发送项目中的词语，不应当在发送项目中的词语，等等。明显地，并且关于发送项目 14 本身，策略可进一步阐述与发送项目 14 有关的，尤其是与可以是对发送项目 14 是否确实是基于所花费的人类努力构造的起决定作用的因素有关的某些参数。在这点上，并且如可意识到的，策略例如可阐述发送项目 14 的最小构造时间，键盘敲击的最小数量，鼠标点击的最小数量，每单位时间发送发送项目 14 的最大数量，等等。据推测，并且应当意识到的，为接收者 16 阐述的策略的每个方面可以针对从发送证明 18 中的陈述获得的信息来测量。

[0054] 在步骤 405 基于策略检查发送证明 18 中的陈述之后，接收者 16 随后基于策略是否实际上由发送证明 18 满足来确定是否实际上承兑发送项目 14（步骤 407）。如应当意识到的，如果策略实际上由发送证明 18 满足，则以任何被认为适当的方式承兑、接受发送项目 14，并且对它行动（步骤 409）。例如，如果发送项目 14 是与接收者 16 相关联的用户的消息，则这样的发送项目 14/ 消息被交付到该用户等的接收区。同样，如果发送项目 14 是对来自接收者 16 或有关实体的服务或对象的请求，这样的发送项目 14/ 请求被交付到可以处理它并提供服务或对象等的服务器等。

[0055] 注意，如果策略实际上没有被发送证明 18 满足，则发送项目 14 被拒绝并 且不被承兑、接受，并且不对它行动（步骤 411）。在这样一个情况下，接收者 16 可向在计算设备 12 处的发送者返回一个简单的拒绝消息、说明拒绝的详细消息等等（步骤 413）。然而，并且尤其是在发送者是某种邪恶实体的情况下，会出现这样的情况，即任何返回消息会带来更多不想要的请求或者其它不想要的注意，并且在这样的情况下这样的返回消息有可能是不可取的。

[0056] 接收者 16 还可在拒绝情况下将该情况通知一拒绝过滤器（步骤 415）。如可意识到的，这样的拒绝过滤器随后可过滤掉来自被拒绝请求的发送者的更多请求。另外或者在替换方案中，接收者 16 也可在拒绝情况下将被拒绝请求的发送者添加到被拒绝发送者列表（步骤 417）。这里，来自该发送者的更多请求将不被过滤掉，但基于在这样的列表上而被不同地对待。

[0057] 结论

[0058] 对于发送一发送项目 14 给接收者的任何适当的发送者，并假定这样的发送者和接收者 16 被适当地配置，可实施本发明。现在应当意识到，有了在此所述的本发明，可用使得发送项目 14 伴随着详述发送者所花费的人类努力的发送证明 18 的方式执行将发送项目 14 发送给接收者。

[0059] 实现结合本发明执行的过程所需的编程是相对简单的，并且对于有关编程技术人员应当是显然的。因此，在本文中不附上这样的编程。然后，可使用任何特定的编程来实现本发明而不脱离本发明的精神和范围。

[0060] 在上述说明中，可以看到本发明包括新的且有用的体系结构和方法用于实现人类交互证据 (HIP)，实质上不需要由人类花费主动努力，而是人类只花费被检测的自然努力。这样被检测的自然努力由可信的证明单元 24 以可信方式向接收者 16 验证，因此可以向接收者 16 保证所检测的自然努力确实是实际发生的并且不是被企图欺骗接收者 16 的恶意实体简单地设计出来的。

[0061] 应当意识到，可在不脱离本发明思想的情况下对上述实施例进行修改。更显然地，

要意识到，本发明不仅可被用于包括人类与发送项目 14 交互的标记，而且还包括与发送项目 14 有关的任何标记，如人类交互、机器交互等等。因而，例如这样一种情况，使用本发明向接收者 16 证明发送应用程序 26 每单位时间没有发送超过最大数量的发送项目 14，无论涉及的任何人类交互。因此，一般应当理解，本发明不限于所揭示的特定实施例，而旨在覆盖由所附权利要求书定义的本发明的精神和范围内的修改方案。

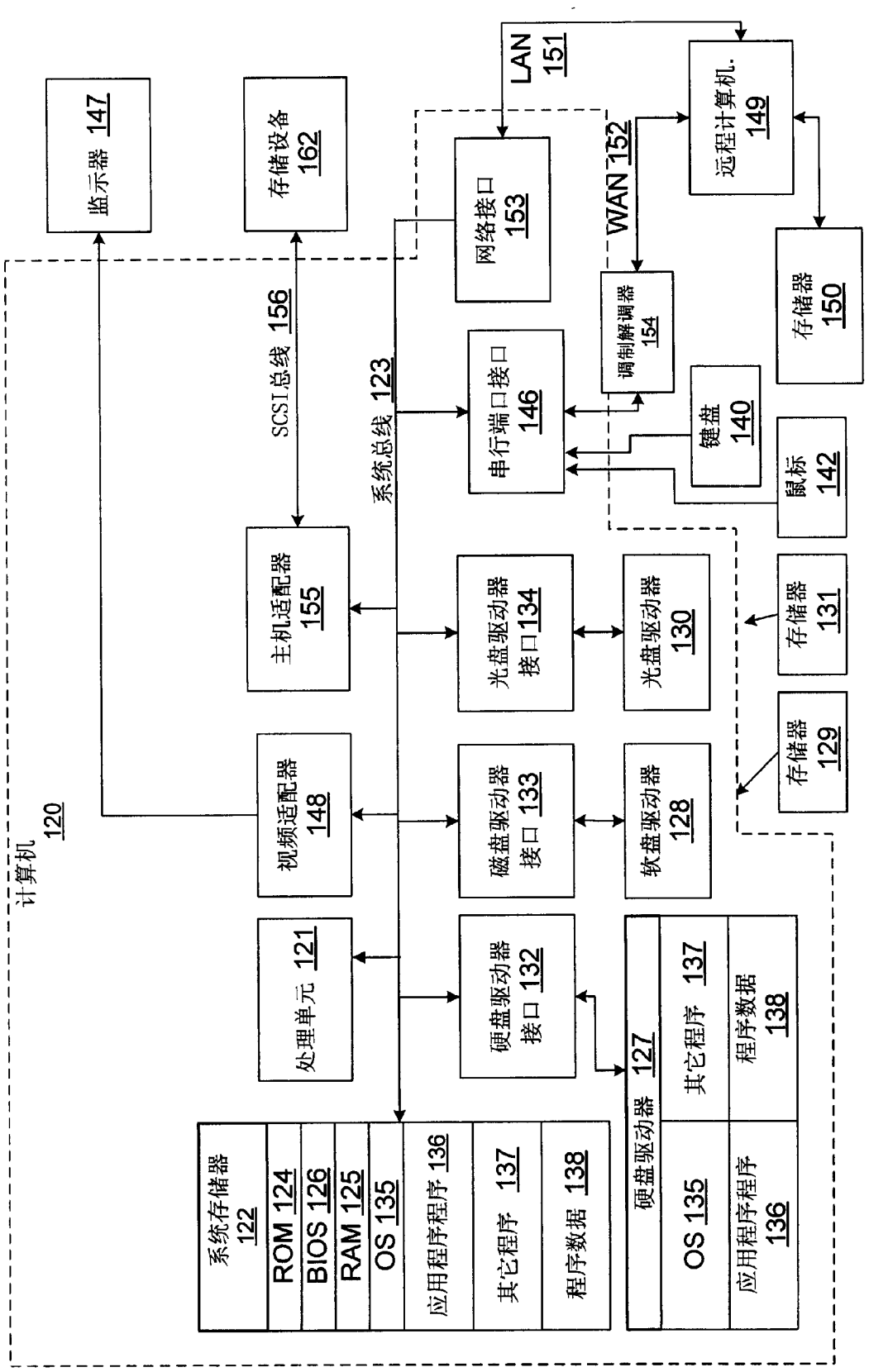

计算机 120
监示器 147
存储设备 162
LAN 151
远程计算机 149
网络接口 153
WAN 152
调制解调器 154
存储器 150
SCSI总线 156
系统总线 123
串行端口接口 146
键盘 140
鼠标 142
主机适配器 155
光盘驱动器接口134
光盘驱动器 130
存储器 131
视频适配器 148
磁盘驱动器接口 133
软盘驱动器 128
存储器 129
处理单元 121
硬盘驱动器接口 132
系统存储器 122
ROM 124
BIOS 126
RAM 125
OS 135
应用程序程序 136
其它程序 137
程序数据 138
硬盘驱动器 127
OS 135
应用程序程序 136
其它程序 137
程序数据 138

图 1

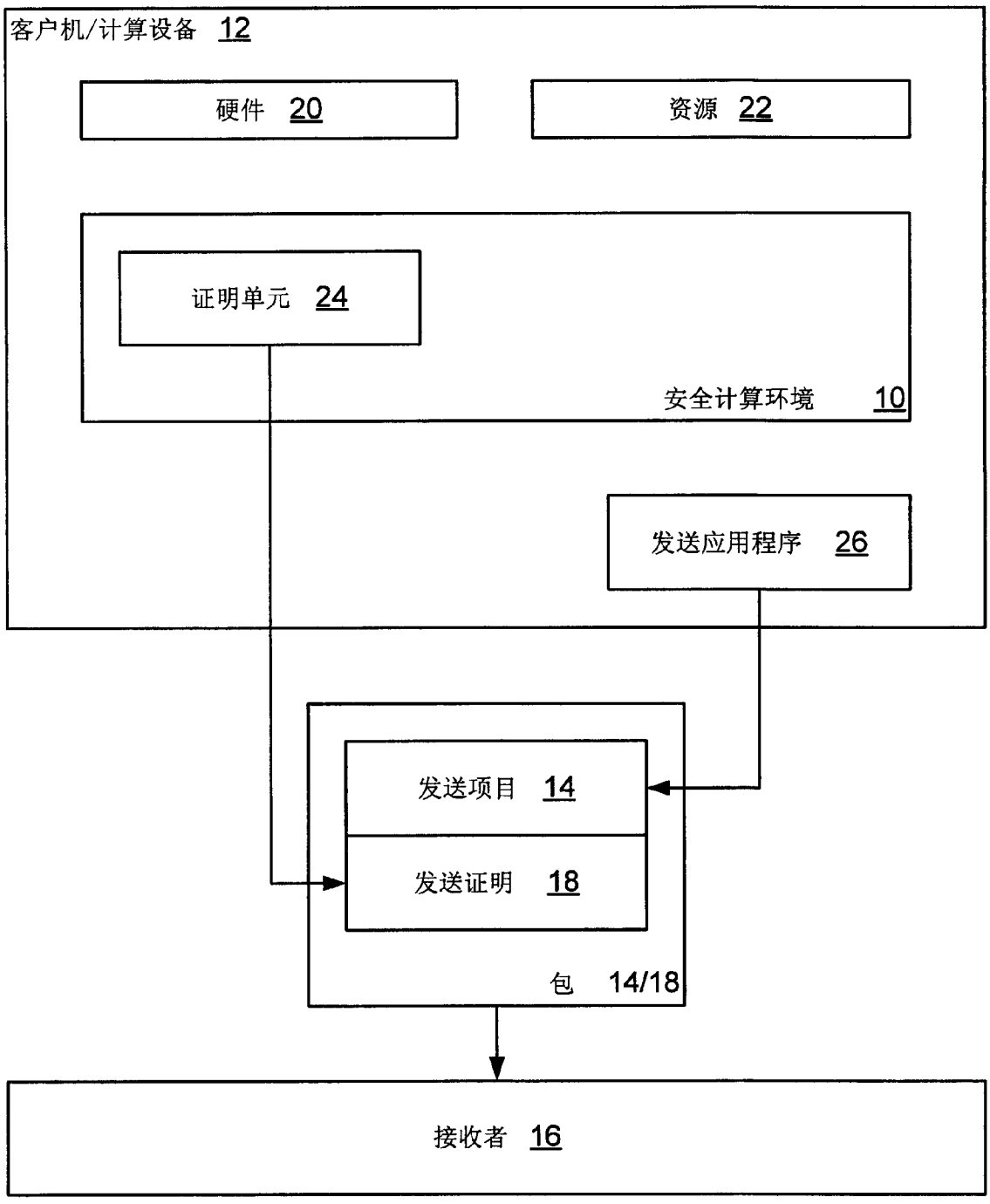

客户机/计算设备 12
硬件 20
资源 22
证明单元 24
安全计算环境 10
发送应用程序 26
发送项目 14
发送证明 18
包 14/18
接收者 16

图 2

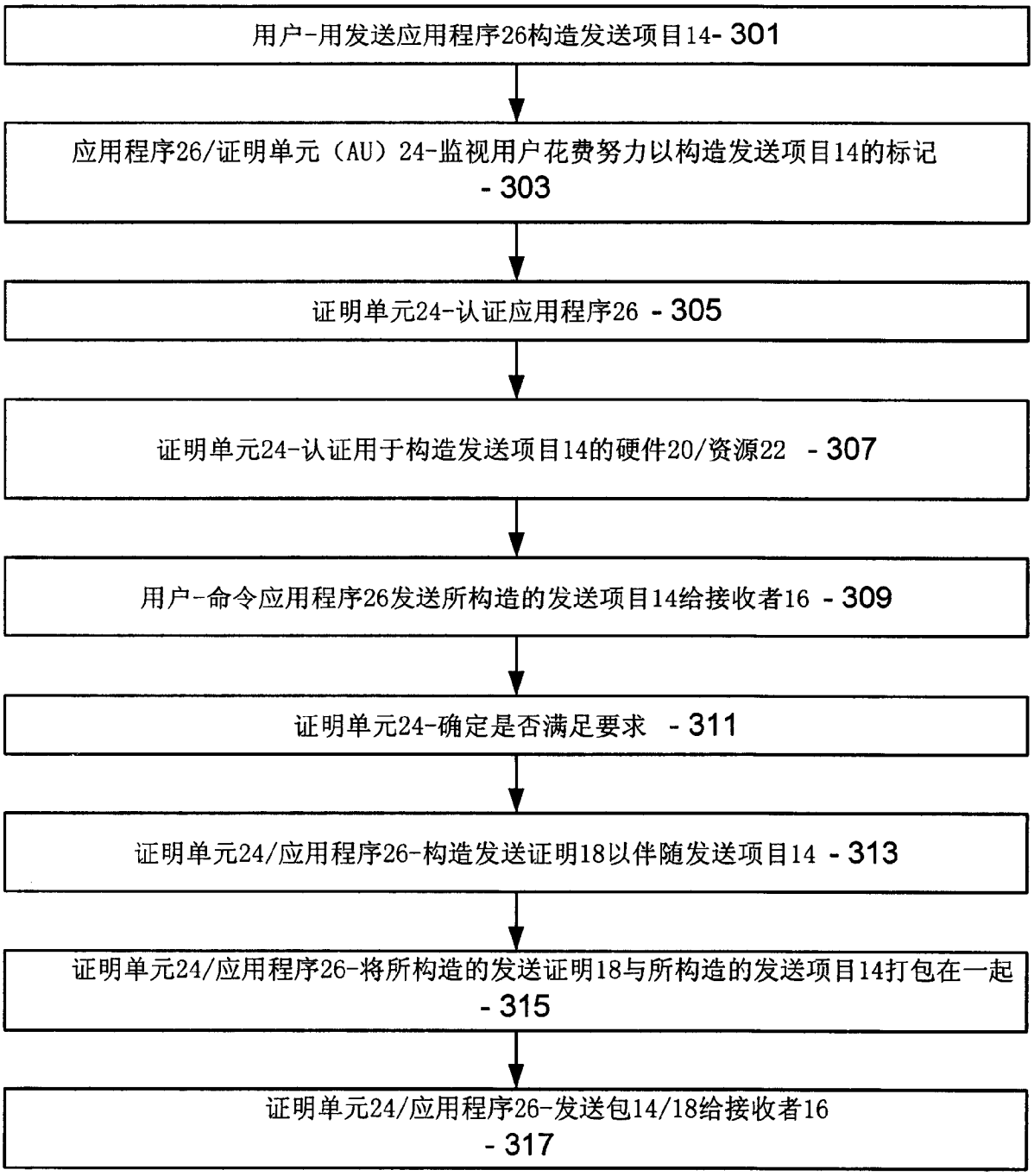

用户-用发送应用程序26构造发送项目14- 301
应用程序26/证明单元（AU）24-监视用户花费努力以构造发送项目14的标记 - 303
证明单元24-认证应用程序26 - 305
证明单元24-认证用于构造发送项目14的硬件20/资源22 - 307
用户-命令应用程序26发送所构造的发送项目14给接收者16 - 309
证明单元24-确定是否满足要求 - 311
证明单元24/应用程序26-构造发送证明18以伴随发送项目14 - 313
证明单元24/应用程序26-将所构造的发送证明18与所构造的发送项目14打包在一起 - 315
证明单元24/应用程序26-发送包14/18给接收者16 - 317

图 3

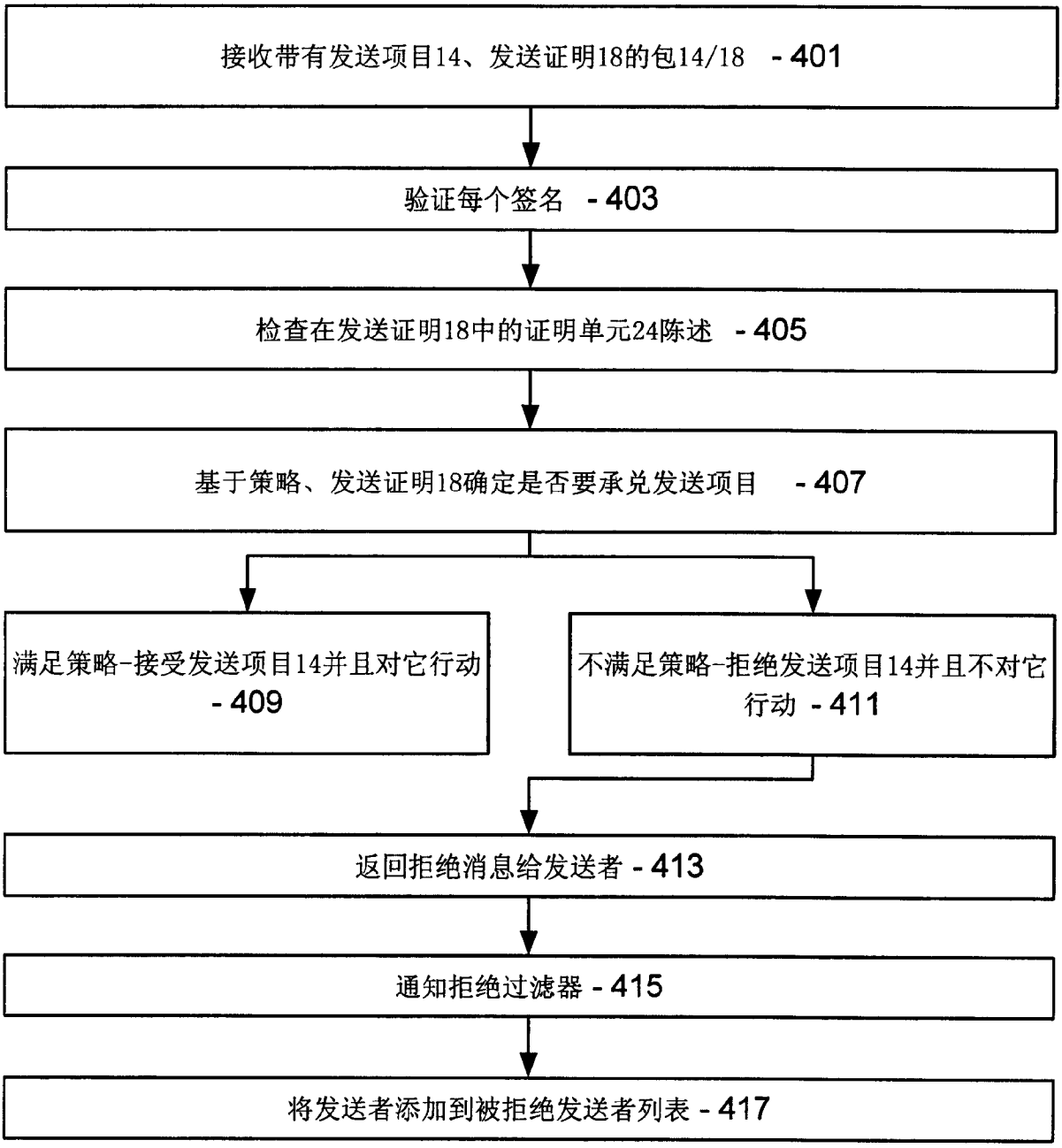

接收带有发送项目14、发送证明18的包14/18 - 401
验证每个签名 - 403
检查在发送证明18中的证明单元24陈述 - 405
基于策略、发送证明18确定是否要承兑发送项目 - 407
满足策略-接受发送项目14并且对它行动 - 409
不满足策略-拒绝发送项目14并且不对它行动 - 411
返回拒绝消息给发送者 - 413
通知拒绝过滤器 - 415
将发送者添加到被拒绝发送者列表 - 417

图 4