[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610172398.2

[45] 授权公告日 2009 年 7 月 22 日

[11] 授权公告号 CN 100517357C

[22] 申请日 2006.10.31
[21] 申请号 200610172398.2
[30] 优先权
[32] 2005.10.31 [33] EP [31] 05110218.4
[73] 专利权人 捷讯研究有限公司
地址 加拿大安大略省沃特卢市
[72] 发明人 罗忠海 布赖恩·R·戈林
迈克尔·申菲尔德
[56] 参考文献
CN1535407A 2004.10.6
EP1434119A2 2004.6.30
US6898706B1 2005.5.24
审查员 赵 婷

[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王 玮

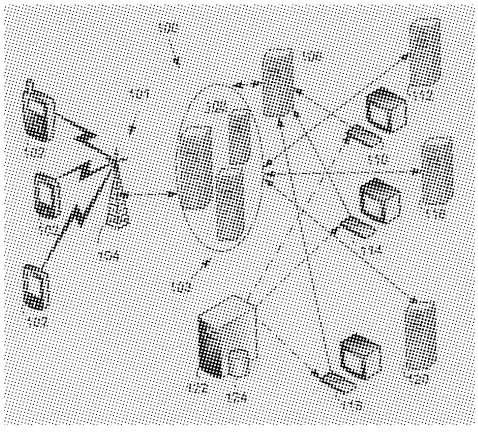
权利要求书 3 页 说明书 13 页 附图 3 页

[54] 发明名称

安全许可密钥方法和系统

[57] 摘要

一种安全许可密钥解决方案为授权和/或追踪软件的使用提供软件许可密钥，其中许可密钥包括由私钥加密的消息和根据非对称加密技术验证该消息的公钥。 该消息和公钥可以由软件授权者(如安装向导)使用，以授权软件和/或生成与软件输出结合的安全标签，从而唯一确定产生该输出的软件的许可。 一种许可密钥管理系统可以为各个软件被许可方生成许可密钥，并包括用于存储各个软件被许可方及其许可密钥之间的关联的数据库，以识别与所获得的输出相关联的许可。



1. 一种为控制软件使用的许可提供安全许可密钥的方法，包括：

为许可生成许可密钥，所述许可密钥包括具有被许可使用软件的被许可方的被许可方信息的散列值的消息，所述许可密钥由私钥签名并可由公钥验证，该私钥和公钥遵照非对称加密技术；

存储至少一个被许可方信息和所述被许可方信息的散列值；

为软件授权者提供许可密钥和公钥，以接收许可密钥并对其进行验证，以授权与该软件授权者相关联的被许可软件的使用；

软件授权者使用公钥和许可密钥生成安全标签，所述安全标签与所述被许可软件的输出相结合，用于随后使用与被许可方相关联的私钥对散列值的解密，以获得被许可方信息；以及

将被许可方信息的散列值与已存储被许可方信息的散列值以及被许可方信息的已存储散列值中的至少一个进行比较，以识别与被许可软件的输出相关联的许可。

2. 如权利要求 1 所述的方法，包括为被许可使用软件的被许可方存储与被许可方信息相关联的公钥和私钥。

3. 如权利要求 1 所述的方法，包括提供软件授权者，所述授权者包括捆绑于所述被授权软件的软件安装器。

4. 如权利要求 3 所述的方法，包括分别根据私钥和许可密钥来提供软件。

5. 如权利要求 2 所述的方法，包括提供软件授权者，所述授权者包括捆绑于所述被授权软件的软件安装器。

6. 如权利要求 5 所述的方法，包括分别根据私钥和许可密钥来提供软件。

7. 如权利要求 1 至 6 中任何一个所述的方法，其中被许可软件包括用于编程组件应用程序的软件。

8. 如权利要求 1 至 6 中任何一个所述的方法，包括对于将要被授权使用被许可软件的被许可方接收被许可方信息，并使用至少部分该被许可方信息来定义消息。

9. 如权利要求 7 所述的方法，包括对于将要被授权使用被许可软件的被许可方接收被许可方信息，并使用至少部分该被许可方信息来定义消息。

10. 一种管理被许可方对软件的使用的许可密钥管理系统，包括：

许可密钥生成器（202），用于：

为许可生成许可密钥（206）以管理被许可软件的使用，许可密钥包括具有被许可使用软件的被许可方的被许可方信息的散列值的消息，所述许可密钥由私钥签名并可由公钥验证，该私钥和公钥遵照非对称加密技术；和

将许可密钥和公钥一起提供给软件授权者，以接收许可密钥并对其进行验证，从而授权被许可方对与该软件授权者相关联的软件的使用；

数据库（204），用于存储许可密钥和与各个被许可方信息中的至少一个和各个被许可使用被许可软件的被许可方信息的散列值相关联的各个私钥/公钥对；以及

许可密钥验证器（214），用于接收来自软件的输出，其中包括与输出结合的安全标签，该安全标签由许可密钥和为授权被许可软件而提供的公钥生成，许可密钥验证器还用于使用与被许可方相关联的私钥，解密散列值，以获得被许可方信息的散列值，并将被许可方信息的散列值与已存储被许可方信息的散列值以及被许可方信息的已存储散列值中的至少一个进行比较，以识别与被许可软件的输出相关联的许可。

11. 如权利要求 10 所述的系统，包括用于生成有关系统使用的管理报告的管理组件（203）。

12. 如权利要求10或11所述的系统，其中许可密钥生成器(202)从一组密钥对中选择私钥和公钥对，为特定许可生成许可密钥(206)。

安全许可密钥方法和系统

技术领域

本发明一般涉及计算机软件分布，并且特别涉及安全许可密钥方法和系统。

背景技术

软件，特别是商业软件，典型地依照一软件许可从一个实体到另一个实体分布。该许可授予软件用户特定的权限。一种依照许可条件来控制软件使用的方式是使用许可密钥，当其适当地与被许可软件相关联时可对软件的安装、执行和/或其它方面进行授权。例如，要安装的被许可软件被捆绑到一个自动软件安装程序或向导以及一许可密钥验证器。在安装期间，验证许可密钥的真实性且作为响应来安装许可软件。许可密钥验证器也可以在启动或尝试使用被许可软件时验证许可密钥。

需要一种安全许可密钥解决方案，以防止他人生成或验证未授权但却在算法上正确的许可密钥。经常地，同样的算法被用于许可密钥生成器和对应的验证器。因为一般验证器被捆绑于软件安装器，恶意的程序员或黑客可轻易地通过逆向工程来确定该算法，并利用该算法建立他/她自己的生成器以创建尽可能多的密钥去模仿正确的许可。

进一步，需要一种灵活的许可密钥解决方案，这样许可密钥管理员（与被许可软件的分布相关联的人，其负责管理许可密钥解决方案）可以轻易地改变许可密钥生成和验证算法所必需的设置，以对不同用途的许可密钥进行分类或分组。

还需要一种易于管理和统计并且可同样访问其它细节的许可密钥解决方案。例如，许可密钥管理员可以要求许可密钥相关的发行报告，诸如多少许可密钥已被发行，多少被许可方已被许可，许可密钥

何时生成、被许可方何时注册等等。

被许可软件可包括开发工具和应用程序，可用于定义和/或发布其它人使用的其它软件或输出。还需要确定哪一个被许可软件产生了特定的输出。

因此，作为结果，需要一种解决这些问题中的一个或多个的方法和装置。

发明内容

本发明涉及一种安全许可密钥解决方案，用于在分布式计算机系统中分布和/或追踪软件的使用。

一种安全许可密钥解决方案为授权和/或追踪软件的使用提供软件许可密钥，这里许可密钥包括由私钥加密的消息部分和根据非对称加密技术验证该消息的公钥部分。该消息和公钥可以由软件授权者（如安装向导）使用，以授权软件和/或生成与软件输出结合的安全标签，从而识别产生该输出的软件许可。一种许可密钥管理系统可以生成许可密钥，并包括用于存储各个软件被许可方及其许可密钥之间的关联的数据库，以对产生所获得输出的软件的特定许可追踪其起源。例如，将被许可的软件可包括编程和输出其它软件的综合开发环境。其它软件的输出可以捆绑于安全标签并为他人使用而发布。这种输出可使用安全标签获得并被追踪其起源（如识别关联许可）。

许可密钥管理系统可适合于生成管理报告等并依照所需加密技术配置许可密钥的产生。

本领域普通技术人员将从说明和描述的实施例中理解本发明的计算机系统、方法、计算机程序产品以及其它方面。

依照一方面，优选地提供一种为控制软件使用提供安全许可密钥的方法，包括：为许可生成一许可密钥，所述许可密钥包括由私钥签名并可由公钥验证的消息，该私钥和公钥遵照非对称加密技术；和为软件授权者提供许可密钥和公钥，以接收许可密钥并对其进行验证，以授权与该软件授权者相关联的被许可软件的使用。

该方法可包括为被许可使用软件的被许可方存储与被许可方信

息相关联的公钥和私钥。

所述方法可包括提供软件授权者，所述授权者包括捆绑于所述被授权软件的软件安装器。

该软件授权者可使用公钥和许可密钥生成安全标签，所述安全标签与所述被许可软件的输出相结合，用于识别被许可软件的许可。同样，该方法可包括使用安全标签识别与该输出相关联的许可。例如，该方法可包括为被许可使用被许可软件的被许可方存储与被许可方信息相关联的公钥和私钥，并使用与被许可方相关联的私钥解密该安全标签。

该被许可软件可包括适于编程组件应用程序的综合开发环境（IDE）。

该方法可包括对于将要被授权使用软件的被许可方接收被许可方信息，并使用至少部分该被许可方信息来定义消息。

依照另一方面，提供一种管理被许可方对软件的使用的许可密钥管理系统，包括：

许可密钥生成器，用于：

为许可生成许可密钥以管理被许可软件的使用，许可密钥包括由私钥签名并可由公钥验证的消息，该私钥和公钥遵照非对称加密技术；和

将许可密钥和公钥一起提供给软件授权者，以接收许可密钥并对其进行验证，从而授权被许可方对与该软件授权者相关联的软件的使用；和

数据库，用于存储许可密钥和与各个被许可使用被许可软件的被许可方信息相关联的各个私钥/公钥对。

根据另一方面，提供一种计算机程序产品，包括计算机可读介质，具体实现了可由计算机执行以进行以下操作的指令和数据：

为许可生成许可密钥，所述许可密钥包括由私钥签名并可由公钥验证的消息，该私钥和公钥遵照非对称加密技术；和

将许可密钥和公钥一起提供给软件授权者，以接收许可密钥并对其进行验证，以授权与该软件授权者相关联的被许可软

件的使用。

附图说明

现在将参考附图，作为示例，对实施例进行描述，其中：

图 1 为说明包括无线和有线通信网络的分布式计算机系统的一个实施例的方框图；

图 2 为更详细地表示图 1 所选择组件和包括用于图 1 的分布式计算机系统中的外部许可密钥的实施例的方框图；

图 3A 和 3B 为根据生成外部许可密钥（如图 2 所示的密钥）的实施例的操作流程图；

图 4 和图 5 为根据一实施例的操作流程图，该实施例示出了外部许可密钥如何用于分布计算机软件以及如何在如图 1 所示的分布式计算机系统中追踪其使用。

具体实施方式

图 1 为表示分布式计算机系统 100 的方框图，其包括通过无线和有线通信网络 101 和 103 连接通信的多个计算设备。系统 100 包括无线移动设备 102（如智能电话、PDA 等类似装置）、无线网络设备 104，组件应用知识库 106、无线应用程序网关系统 108、多个数据源 112、116、120、软件开发站 110、114 和 118、以及包括安全数据存储 124 的许可密钥生成和验证系统 122。

连同参考图 2 并简要说明，计算机系统 100 使用软件开发站（如 110、114、118）所开发并发布到知识库 106 的组件应用程序（如 218）方便数据在移动设备 102 和数据源 112、116 以及 120 之间通信。软件开发站 110、114、118 包括软件开发工具，例如综合开发环境（IDE）（如站 110 中的 216），其为程序员而配置为产生包括安全 IDE 标签 218 的组件应用程序。该安全 IDE 标签用于为用作创建组件应用程序的软件确定其许可。通过提供实体或代表提供实体，将 IDE 的实例（如 216）分发给想要开发组件应用的其他人（即“被许可方”）。IDE 的授权处于许可密钥（如 206）生成和验证系统 122 所生成的各个安全许可密

钥的控制之下。该安全许可密钥（如 206）是依照非对称加密技术（如 RSA 算法）由公钥和密钥对生成的，其基于各个被许可方信息而安全存储于许可密钥数据库 204，以使安全许可密钥生成并进一步确认与组件应用程序相关联的许可。

移动设备 102 在无线网络设备 104 中并通过无线网络设备 104 进行通信。在图 1 实施例的示例中，无线网络 104 是基于码分多址（CDMA）技术的第三代（3G）支持网络。特别地，无线网络 104 是 CDMA2000 网络，其包括如图 1 所示的方式进行连接的固定网络组件。CDMA2000 类型的无线网络 104 可包括无线电网络（RN）、移动交换中心（MSC）、7 号信令（SS7）网络、归属地位置寄存器/鉴权中心（HLR/AC）、分组数据服务节点（PDSN）、IP 网络、以及远程验证用户拨入服务（RADIUS）服务器（未全部示出）。SS7 网络通信连接于诸如公共交换电话网（PSTN）的网络以进行语音通信，而 IP 网络通信连接于诸如互联网的网络以进行特定数据通信。无线网络 104 为示例性且本领域普通技术人员将意识到其它无线网络结构和标准也可使用。

图 1 的通信系统 100 中所示的无线连接表示一个或多个不同的信道，典型地为不同的射频（RF）信道，以及用于无线网络 104 和移动设备 102 之间的相关协议。本领域技术人员将意识到实际使用的无线网络可根据所需全部网络覆盖区域包括数百个发射区。所有相关组件可以被多个交换机和路由器（未示出）连接，并由多个网络控制器所控制。

本领域技术人员将意识到无线网络 104 可连接于其它系统，可能包括其它网络，其未在图 1 中明确示出。尽管需要 CDMA 无线网络 104，然而网络 104 可遵照包括蜂窝网、广域网络、GSM、GPRS、CDMA、iDEN™、Mobitex™等在内的任何无线网络技术和协议。

移动设备 102 典型地为多任务无线通信设备，其被配置为发送和接收诸如电子邮件、即时消息、SMS 消息以及其它数据消息的数据，并至少部分地被配置为发起或接收语音呼叫。为了提供用户友好的环境以控制移动设备 102 的操作，驻留在设备 102 上的操作系统（未示出）提供一用户界面，例如具有主屏幕和多个可从主屏幕导航的子屏

幕的图形用户界面（GUI）。

同样在当前实施例中，移动设备包括一运行时间环境，用于为与诸如数据源 112、116 和 120 的数据源通信提供服务和运行组件应用程序。

数据源可包括具有外露程序界面的应用程序，该外露程序界面用于依照面向服务的结构（如网络服务协议）与其它应用程序通信。这种服务典型地但不是必须地为基于订阅的。

无线组件应用程序网关系统 108 便利了移动设备 102 和数据源之间的通信。虽然没有示出，但网关系统 108 包括组件应用程序网关、组件应用程序供应服务器以及组件应用程序发现服务器。该组件应用程序网关用于代理由数据源提供给移动设备的服务，例如映射无线和有线协议之间的通信。

发现服务器能够使移动设备定位新的或升级的服务并通过供应服务器从组件知识库 106 获得相关组件应用程序。

应用程序以包或束的集合的形式存储在组件知识库 106 中。包典型地由应用程序开发者使用开发环境所提供的设计工具生成，该开发环境有时被称为 IDE。IDE 典型地为拖放图形方法提供支持用于包括屏幕、数据元素、消息和应用程序工作流逻辑的应用程序组件的可视设计，其接下来被进一步定义。应用程序包优选地由结构化数据（XML）表示，该结构化数据可由 IDE 通过一自动代码生成过程自动生成。设计工具进一步能够使自动生成代码包括产业标准脚本语言（如 JavaScript）或本领域所知的其它脚本/编程语言，或者以另外的方式由该产业标准脚本语言或本领域所知的其它脚本/编程语言进行增补。知识库 106 中的应用程序包的可用性通过由发现服务器提供的发现服务发布于一注册记录中。可以认识到，该网关服务器可以使用多于一个的知识库 106 以及与其关联的注册记录。

程序员可以通过与所描述的 IDE 相适应的站 110、114 和 118 编程组件应用程序从而将服务扩张到移动设备。在一个实施例中，这样的 IDEs 可由一组针对一般综合设计环境的插件程序构成，例如可以是 Eclipse™构架。Eclipse™构架是众所周知的开发环境，且这些和其

它特征在 www.Eclipse.org 被详尽描述。作为代替，工具可被配置为不使用插件程序结构的完全设计构架。仅为了示例性用途，工具在此被描述为一使用 Eclipse™构架的插件程序设计环境。

参考图 2，主要描述了设计组件应用程序的 IDE 216 。在当前实施例中，设计者工具使用 Eclipse™实现。Eclipse™被设计为支持多种用于应用程序环境的工具的构造。进一步，Eclipse™支持一组不受限的工具提供者，包括独立软件卖方（ISV）以及用于操作随机内容类型的工具（例如 HTML、Java、 C、 JSP、EJB、XML 和 GIF）。Eclipse™支持基于 GUI 和非 GUI 的应用程序开发环境。如接下来进一步描述的，IDE 适于包括安全标签插件，以包括发布的应用程序中的安全标签。

在当前实施例中，IDE 216 用于使开发者定义一组件应用程序。组件应用程序一般是由一组结构化组件所定义的，结构化组件包括数据组件、消息组件、表示组件和工作流组件。组件使用结构化语言定义，并由智能运行时间容器在客户设备上执行。

数据组件定义由组件应用程序使用的数据实体。数据实体的例子包括订单、用户和金融交易。数据组件定义描述数据实体所需的信息以及信息表达的格式。例如，数据组件可定义一订单，其包括数字格式的唯一的订单标识符、串格式的一列项目、具有日期-时间格式的订单建立时间、串格式的订单状态以及根据另一个数据组件定义而格式化的发出订单的用户。由于数据元素通常经消息传递，故此数据组件经常存留在数据库中。数据组件可由应用程序设计者动态生成或定义。

消息组件定义消息的格式，组件应用程序使用该消息与诸如网络服务的外部系统进行通信。例如，一个消息组件可描述一个发出订单的消息，其包括唯一的订单标识符、订单状态以及与订单相关的注释。

表示组件在组件应用程序通过用户界面显示给用户时定义其外观和行为。表示组件能够指定图形用户界面（GUI）屏幕，并且用户与组件应用程序互动时可执行其控制和动作。例如，表示组件可定义屏幕、标签、编辑框、按钮和菜单以及当用户在编辑框中键入或按动按钮时所执行的动作。

组件应用程序的工作流组件定义当一个动作将要被执行时所发

生的处理，这样的动作由上述表示组件指定，或者定义当消息到达时所要执行的动作。表示工作流和消息处理由工作流组件定义。工作流组件以结构化数据、编程语言或脚本语言被写为一系列指令。工作流组件支持消息组件间的相关性，并将应用程序流定义为在其它组件上操作的一组规则。

关于组件应用程序更多的细节可见专利合作条约申请号为PCT/CA2003/001976的、题目为“System and Method for Building and Execution of Platform-Neutral Generic Services Client Applications”的专利申请，其公开号为WO2004059938；专利合作条约申请号为PCT/CA2003/001980的、题目为“System and Method of Building Wireless Component Applications”的专利申请，其公开号为WO2004059957；专利合作条约申请号为PCT/CA2003/001981的、题目为“System and Method of Creating and Communicating with Component Based Wireless Applications”的专利申请，其公开号为WO2004059939，其中每个申请都属于本申请的申请人。

面向服务的协议主要针对有线网络通信而定义，基于组件应用程序的体系结构提供了许多功效，其中组件应用程序网关系统代理代表移动设备的数据源。服务经常处理敏感的通信（商业交易、私人信息等）。这样，迫切需要一种识别软件许可的机制以用于生成组件应用程序的编程，其可进一步用于识别特定的被许可方以及在系统100内交换信任。

图3A描述了诸如使用许可密钥生成器/验证器202和数据库204生成外部许可密钥206的操作300的流程。许可密钥生成器/验证器采用包括秘密私钥和对应公钥对来加密数据的非对称加密技术。这样的加密技术是本领域所知的并且其商业实施例可从RSA安全有限公司和其它地方得到。密钥对关联于被许可方，用于生成唯一的且因此可追踪的许可密钥，就如进一步需要的那样。如果需要，一个特定的被许可方可与多于一个的密钥对相关联。

在步骤302，接收被许可方信息（如由许可密钥管理员输入生成器/验证器）。该信息典型地包括被许可方的名称（如公司和联系人）、

地址、所需许可数目等。在步骤 304，确定是否为被许可方建立了一个加密密钥对。数据库 204 可用于对这些信息的查询。如果没有密钥对，通过分支到达步骤 306，生成一个密钥对。可理解的是，预先生成的密钥对池是可用的，从而所述生成包括从该密钥对池中选择一个密钥对。否则，可使用生成算法创建一个新的密钥对。密钥对与被许可方相关联地存储在数据库 204。在步骤 308，从安全存储（数据库 204）中选择一个密钥对。该安全存储或数据库可作为密钥对池使用，管理员能够选择一个密钥对为被许可方定义一个许可密钥。如果需要，不同的被许可方可关联于相同的密钥对。

基于在步骤 308 选择的密钥对，在步骤 310，创建一个内部许可密钥 212（即一个数据组件），并且在步骤 312，创建一个外部许可密钥 206。外部许可密钥记录在数据库中并被分配给被许可方，用于在许可密钥验证器 214 的控制下将 IDE（如 216）安装在被许可方的编程站（如 110）上。

根据一个实施例，外部许可密钥 206 包括内部许可密钥 212、被许可方的私钥/公钥对中的公钥组件 210 和用于为数据组件 206 划定界限的公钥长度模块 208（见图 2）。根据一个实施例，内部许可密钥包括由许可密钥生成器/验证器进行数字签名的唯一识别数据。

图 3B 描述了用于生成内部和外部许可密钥的操作 310 和 312 的一个实施例。在步骤 320，选择被许可方信息定义一消息，用于采用散列函数（诸如 MD5 或 SHA-1）进行编码以生成唯一（为了所有实用的目的）对应于该消息的数据输出。该散列输出根据本领域普通技术人员所知的技术使用密钥对中的私钥进行签名。因此，该签名的散列输出唯一对应于消息和用于创建其的私钥。

该签名的散列输出可定义内部许可密钥 212，与私钥相对应的公钥 210 和公钥数据长度 208 相结合（如相级联），用以生成外部许可密钥 206。为了容易电存储或分配，外部许可密钥 206 优选地被编码，例如使用诸如 Base64 等本领域熟知的编码方法编码为字符串。

外部许可密钥 206 可与被许可软件一起（即同时）或分别被分布，进而被安装或解锁（如 IDE 216）。分布（由图 1 中的虚线表示）可以

为电的，例如通过载波信号上的网络传输；或分布在物理介质上，例如 CD/DVD、固件、软件保护器（dongle）或其它产品。可理解为分布是指点对点的，由此被许可方可接收它的并仅为它的预期许可密钥。

图 4 描述了验证许可密钥和生成安全的 IDE 标签的操作 400。在步骤 402，外部许可密钥被解码（如根据 Base64）。公钥和内部许可密钥被分别提取（步骤 404）。在步骤 406，使用公知的公钥验证内部许可密钥的真实性。例如，公钥被应用于内部许可密钥以确定由许可密钥提供者（典型地为软件许可颁发者）生成的消息散列。验证器 214 也能够对相同的被许可方信息进行散列，并比较两个散列以确定任何篡改。所选择的被许可方信息或消息可在发送给被许可方时捆绑于被许可软件，或者由被许可方在注册期间进入，这样反过来电子地使被许可方信息进入系统 122 以及之前参考图 3A 和 3B 描述的接收并使用该信息生成许可密钥的密钥生成器/验证器 202。

作为选择，尽管没有示出，如本领域已知的那样，一个可信赖第三方可以验证公钥。

在步骤 408，使用公钥生成一个安全的 IDE 标签。使用公钥加密消息散列以定义标签。为了追踪的目的，该标签被插入被许可软件的输出中。

在图 1 和 2 的实施例中，被许可软件为用于编程（即定义和表达诸如我所写的代码和/或数据）其它软件的 IDE 216。其输出包括组件应用程序制造物（如组件定义、数据、脚本、用户界面等），这些被捆绑以发布给知识库 106。组件应用程序包可由此包括 IDE 标签，其专门且安全地识别生成包的 IDE。

图 5 描述了用于追踪已发布应用程序的操作 500。在步骤 502，由许可密钥生成器/验证器 202 获得已发布应用程序，例如从知识库 106 获取。安全的 IDE 标签在步骤 504 被提取用于验证。验证/确定可如接下来描述的那样完成。在步骤 506，使用发布应用程序或其关联程序（如知识库）中存在的被许可方信息（该信息可能不完全相同地对应于之前描述的用于生成消息的被许可方信息），获得数据库 204 中的与被许可方关联的一个或多个私钥。对于每个候选私钥，利用私钥

解密安全 IDE 标签以获取信息散列。这个信息散列被与从数据库 204 中获取的被许可方信息散列相比较，或与之前，例如在许可密钥生成时，生成并存储于数据库 204 中的散列相比较；该消息散列为了上述用途而被实时的生成。尽管不是完全理想的有效，但如果可能的候选者私钥不能由被许可方或其它信息而确定，步骤 506～510 可基于安全数据存储中的所有可能的已知私钥而重复。

如果许可不能由诸如通过操作 500 的输出的安全标签而确定，该输出可被认为是恶意的并被采取适当的行动。例如，被认为是恶意的已发布应用程序可被隔离和重新检查。

许可密钥管理功能 203 可以通过软件提供用于管理数据库 204，并生成各种使用报告和其它统计或存储于其中的特定获取信息。这种功能还可配置许可密钥生成器/验证器 202 以使许可密钥管理员将许可密钥分类或分组。

尽管图 2 仅描述了客户信息与私钥/公钥对相关联的存储于数据库 204，但其它信息也可以被存储。例如，散列算法参考目录可相对于每个客户密钥对被存储，其用于指示哪一个算法被用于生成特定许可密钥。已生成消息的散列或内部许可密钥和/或外部许可密钥也可以被存储。私钥/公钥对生成/验证算法以及密钥和注册的时间和日期信息等也可以被存储。

尽管被作为明确区分的组件而进行描述，本领域普通技术人员将意识到各个操作可在不同软件部件中共享或交迭，并且这样的部件区分可以是人为的。

尽管参考为系统 100 生成组件应用程序而进行描述，本领域普通技术人员将意识到其中的教导使他们轻易地将其用于其它 IDE 软件、工具或应用程序（如单词处理、图形 CAD/CAM、发布等），由此可以为了追踪能力而为这些其它软件输出中的包含物生成安全标签。在此描述的安全许可密钥的生成和验证特征和/或许可密钥管理特征也可被引入不需要安全标签用于追踪的情形。

由于同样的算法被用于许可生成器和验证器代码，而这代表着安全威胁，所以对称加密方法具有严重的缺陷。在非对称方法中，使用

非对称加密算法（如 RSA）生成公钥和私钥对。私钥由软件认可证颁发者保存在安全场所。该私钥被用于为被许可方生成许可密钥，而公钥则依附于已许可软件的安装器并用于在安装期间验证被许可方的许可密钥。这样，即使黑客知晓如何生成和验证许可密钥，由于他/她没有私钥，他/她仍然不能破坏我们的软件保护。

所描述的许可密钥解决方案同样促进了其灵活性。如果公钥是硬编码于安装器中而不是随许可密钥提供，由于将来难以改变私钥和公钥对，则一个旧的安装器不能验证由新的私钥所生成的新的许可密钥。根据该许可密钥解决方案的实施例，一种创新的解决方案能够针对这一问题。将许可密钥（在此表示“内部许可密钥”）与对应的公钥相结合，与公钥配对的私钥用于对该内部许可密钥进行签名，以形成按照 Base64 格式编码的“外部许可密钥”，所述外部许可密钥可由所述公钥进行验证。因此，公钥/私钥对和被许可方之间的关系被记录在许可密钥管理系统的数据库中。外部许可密钥接着被提供给被许可方。在安装期间，软件安装器从外部许可密钥中提取公钥和内部许可密钥，并验证该许可密钥。这种灵活的方法使许可颁发者能够选择不同的公钥/私钥对为不同的终端用户或不同的被许可方组生成许可密钥。

在被许可软件产生的输出可被获取以重新检查的特定情形，追踪能力使得许可颁发者能够将输出追回产生它的被许可软件（追回到一个或一组已知的软件拷贝）。一种直接的方法为将外部许可密钥包括于已许可软件的输出中。但是这种解决方案是有问题的。外部密钥的流通可使得恶意开发者使用不能被适当追踪的其他开发者的信息生成输出。这样可能为攻击者提供可利用的机会，攻击者可从已发布的应用程序获得被许可方的外部许可密钥并猜测被许可方的用户名称和公司名称等，以假冒被许可方安装被许可软件的拷贝并使用其产生诸如发布部件应用程序的输出。

在所提出的许可密钥解决方案的实施例中，在已许可软件的安装期间，被提取的公钥被用于对来自内部许可密钥的数据进行加密，而作为结果的字节流，在此称为“安全 IDE 标签”或更一般的称为“安全标签”，被存储供已许可软件使用。当被许可方产生输出，特别是用于向他人发

送或由他人使用的输出，例如通过经由 IDE 发布一组件应用程序，该安全标签被嵌入所发布应用程序输出。通过使用许可颁发者持有的对应私钥解密安全标签，并将其与内部许可密钥的消息数据相比较，许可颁发者可轻易获知是谁创建并发布了应用程序。

通过许可密钥管理系统的综合管理功能，许可颁发者能够轻易创建报告，诸如多少许可密钥已被发行，数据库中存有多少被许可方，许可密钥何时生成、被许可方何时注册等等。

本申请的上述实施例仅用于举例。在不背离本发明的范围的前提下，本领域技术人员可以对特定实施例的进行改造、修正和变化。所附权利要求中所描述的主题内容倾向于覆盖和包含所有适当的技术改动。

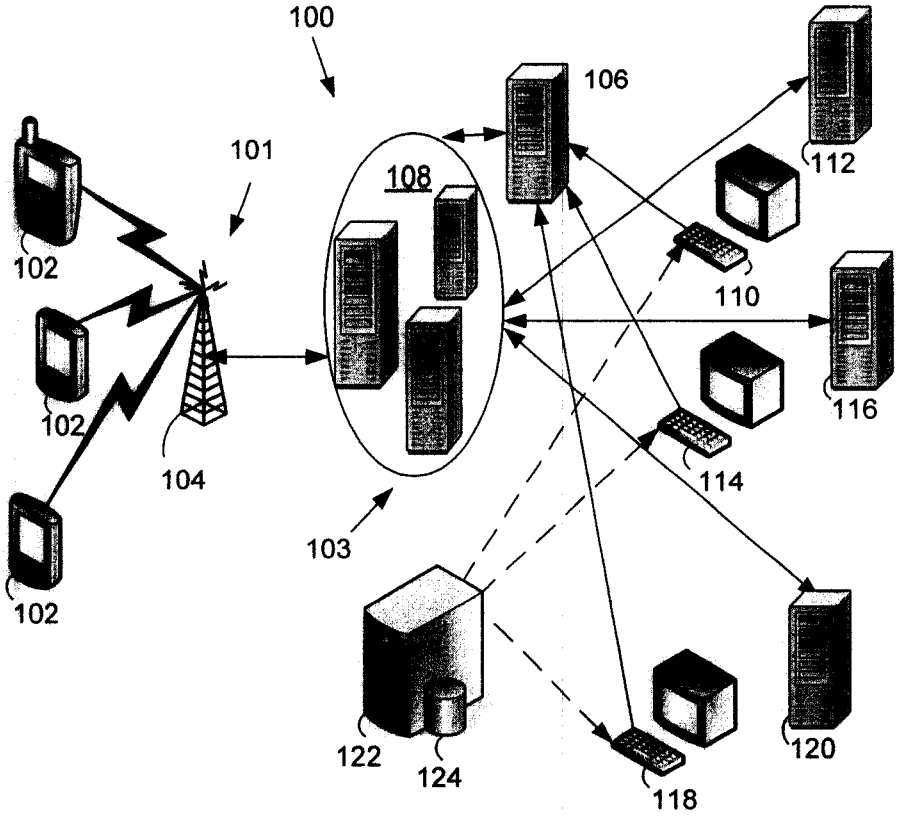

100
101
102
102
102
104
103
106
108
110
112
114
116
118
120
122
124

图 1

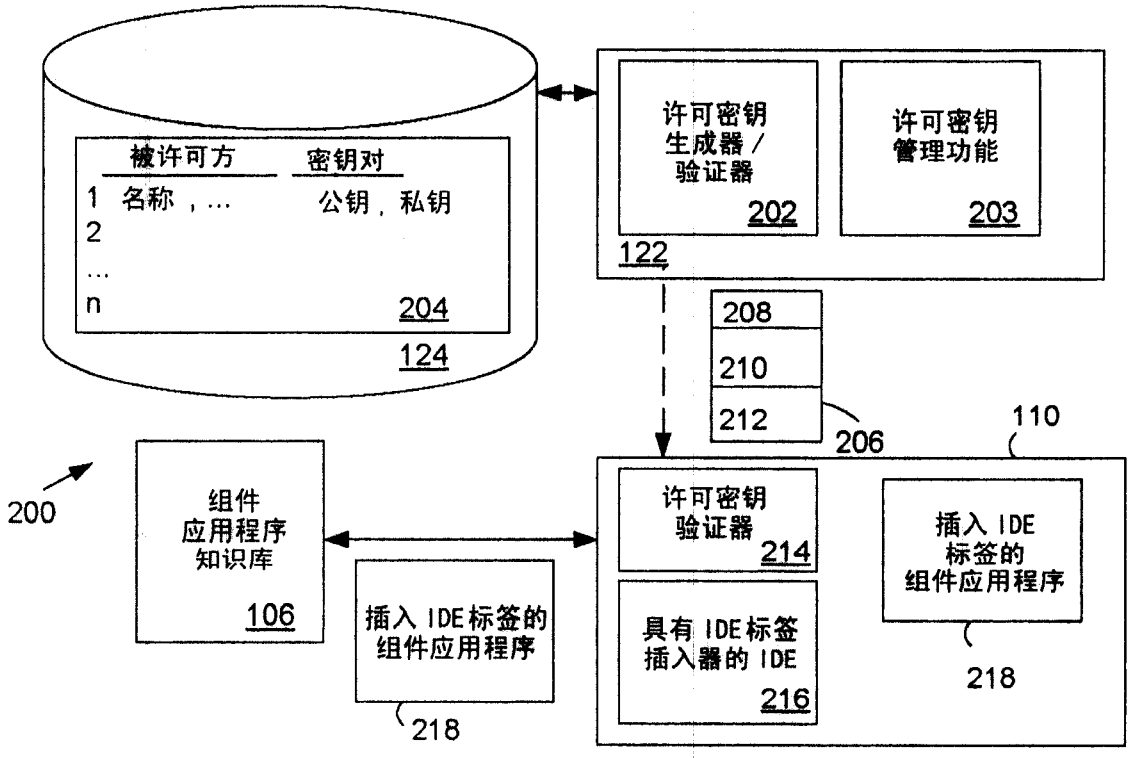

被许可方
密钥对
1 名称，…
公钥，私钥
2
…
n
204
124
许可密钥
生成器/
验证器
202
许可密钥
管理功能
203
122
208
210
212
206
110
200
组件
应用程序
知识库
106
插入 IDE标签的
组件应用程序
218
许可密钥
验证器
214
具有 IDE标签
插入器的 IDE
216
插入 IDE
标签的
组件应用程序
218

图 2

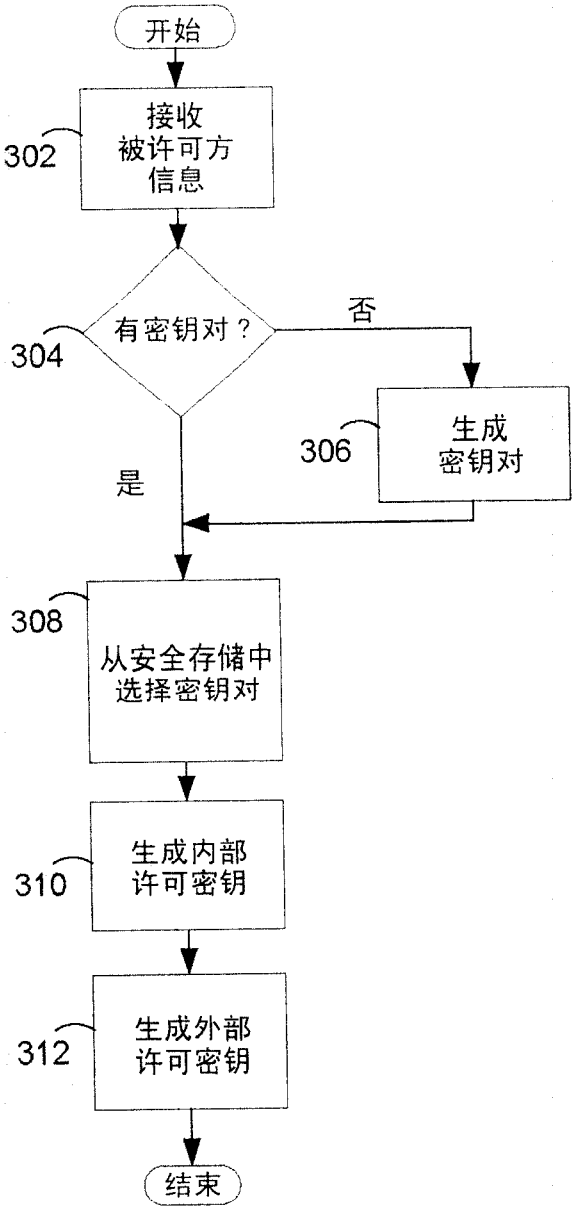

开始
接收
被许可方
信息
302
有密钥对？
304
否
是
生成
密钥对
306
从安全存储中
选择密钥对
308
生成内部
许可密钥
310
生成外部
许可密钥
312
结束

图 3 A

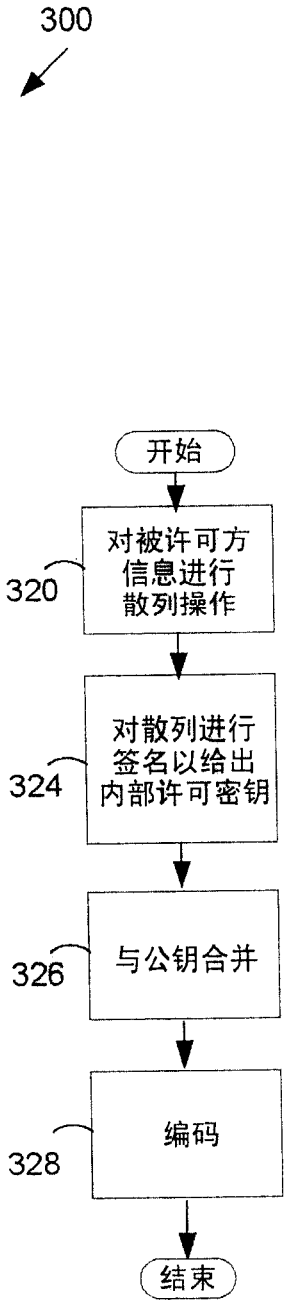

300
开始
对被许可方
信息进行
散列操作
320
对散列进行
签名以给出
内部许可密钥
324
与公钥合并
326
编码
328
结束

图 3 B

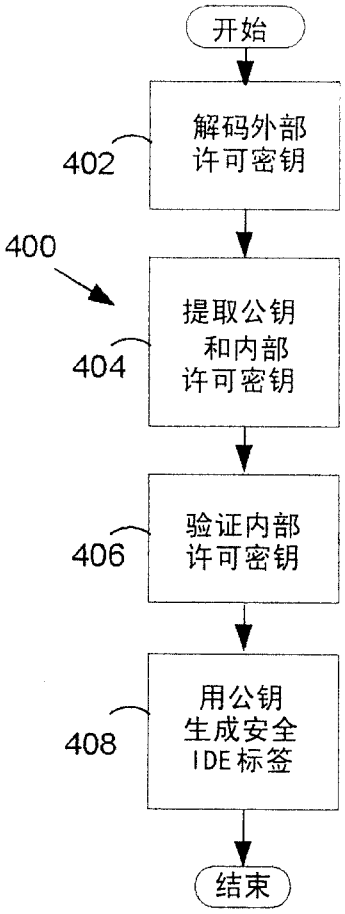

开始
解码外部许可密钥
402
400
提取公钥和内部许可密钥
404
验证内部许可密钥
406
用公钥生成安全IDE标签
408
结束

图 4

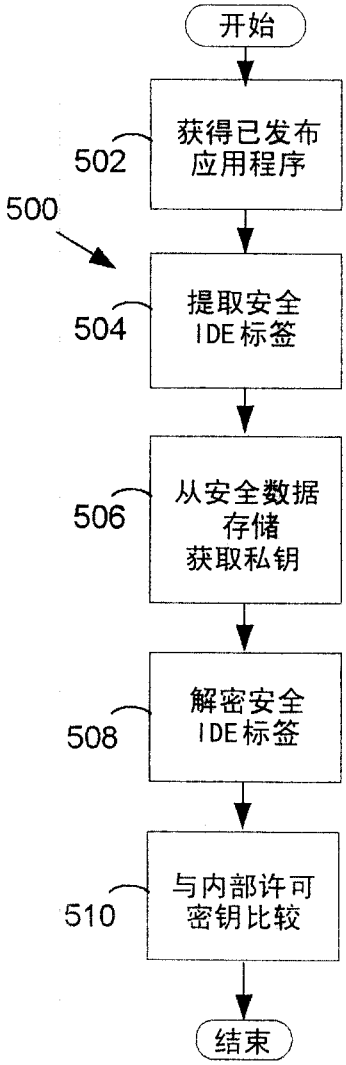

开始
获得已发布应用程序
502
500
提取安全IDE标签
504
从安全数据存储获取私钥
506
解密安全IDE标签
508
与内部许可密钥比较
510
结束

图 5