



(12) 发明专利

(10) 授权公告号 CN 101145257 B

(45) 授权公告日 2012.07.25

(21) 申请号 200710153701.9

(22) 申请日 2007.09.14

(30) 优先权数据

11/521,712 2006.09.15 US

(73) 专利权人 NCR 公司

地址 美国俄亥俄州

(72) 发明人 亚历山大·W·维托克

迈克尔·J·尼兰 詹姆斯·亨德森

(74) 专利代理机构 上海脱颖律师事务所 31259

代理人 脱颖

(51) Int. Cl.

G07F 7/00 (2006.01)

审查员 王建良

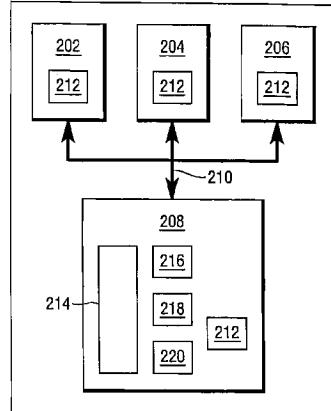
权利要求书 2 页 说明书 4 页 附图 4 页

(54) 发明名称

机器组件的安全验证

(57) 摘要

本发明公开了一种验证自助服务终端中的机器组件的方法，该方法包括提供至少一个带有机器可读标识符的机器组件并且使用处理单元从机器可读标识符中读取标识数据。将该标识数据与处理单元存储器中所存储的标识数据进行比较，以确定组件的标识是否已改变。如果标识已改变，那么处理单元将标识数据与来源数据进行比较，以确定组件是否来自受信任的来源。在一个实施例中，自助服务终端是自动取款机(ATM)，而组件是加密个人识别码(PIN)键盘，现金给付单元和读卡器。



1. 一种在自助服务终端中验证机器组件的方法,包括:
提供至少一个带有机器可读标识符形式的标识信息的机器组件;
从机器可读标识符中读取标识数据;
将该标识数据与存储的标识数据进行比较,以确定组件的标识是否已改变,其中,所述存储的标识数据在首次启动之前从原始组件接收并存储在存储器中;
在每次后续启动中,比较机器组件的标识数据和存储的标识数据以确定组件的标识是否已改变;以及
如果该标识已改变,将该标识数据与来源数据进行比较,以确定该组件是否来自受信任的来源;
在所述终端启动时执行以上步骤;以及
如果新的组件不是来自受信任的来源,禁用所述终端。
2. 如权利要求 1 所述的方法,该方法包括:如果所述标识已改变,并且已证明新组件来自受信任的来源,则使用来自该新组件的标识数据替换所述存储的标识数据。
3. 如权利要求 1 所述的方法,该方法包括在用改变的标识数据替换存储的标识数据之前验证安全数据的步骤。
4. 如权利要求 1 所述的方法,该方法进一步包括,在比较机器组件的标识数据与存储的标识数据后,如果确定组件的标识数据没有发生改变,则完成所述终端的启动。
5. 如权利要求 1 所述的方法,该方法进一步包括,如果所述新的组件来自受信任的来源,由工程师输入安全数据以确保新组件的安装是经过授权的人员完成的。
6. 一种自助服务终端的处理单元,包括:存储器,用于在所述自助服务终端首次启动之前存储从原始组件接收的标识数据,请求装置,用于向该终端的组件请求标识数据,以及比较装置,用于在每次后续启动中,将所述请求装置所接收的组件的标识数据与存储在所述存储器中的从所述原始组件接收的标识数据进行比较以检测标识数据中的任何变化。
7. 如权利要求 6 所述的处理单元,其中所述存储器包括组件的来源数据,并且安排所述比较装置对改变的标识数据与所述来源数据进行比较以确定所述组件是否来自受信任的来源。
8. 如权利要求 6 所述的处理单元,该处理单元还包括安全装置,用来接收来自维护操作人员的安全数据,并使用该安全数据来确定该维护操作人员是否是被授权的操作人员。
9. 如权利要求 6 所述的处理单元,该处理单元被安排为仅当该组件来自受信任的来源的时候才允许与其相关联的终端运行。
10. 一种自助服务终端,包括自助服务终端处理单元,该处理单元包括存储器,所述存储器用于在所述自助服务终端首次启动之前存储从原始组件接收的标识数据,请求装置,用于向该终端的组件请求标识数据,以及比较装置,用于在每次后续启动中,将该请求装置所接收的所述组件的标识数据与存储在该存储器中的来自所述原始组件的标识数据进行比较以检测标识数据中的任何改变,所述自助服务终端还包括带有相关联的标识数据的下列组件中的至少一个:加密 PIN 键盘、现金给付单元和读卡器,安排所述终端使得与每个组件相关联的识别数据可被所述处理单元读取。
11. 如权利要求 10 所述的自助服务终端,该自助服务终端包括每种所述组件中的一个,所述处理单元被安排用于确定每个所述组件是否来自受信任的来源,并且仅当所有的

所述组件都来自受信任的来源时才允许所述终端运行。

12. 如权利要求 10 所述的自助服务终端, 其中每个所述组件包括标识芯片, 与每个组件相关联的标识数据被设置在每个所述组件的标识芯片上。

13. 如权利要求 10 所述的自助服务终端, 该自助服务终端是自动取款机, 其中, 如果比较装置检测到所述标识数据已改变, 所述比较装置将该标识数据与来源数据进行比较, 以确定所述组件是否来自受信任的来源, 并且如果证明所述组件来自受信任的来源, 则使用来自该组件的标识数据替换所述存储的来自所述原始组件的标识数据。

机器组件的安全验证

技术领域

[0001] 本发明涉及自助服务终端 (SST) 中组件的安全验证，尤其涉及，但不局限于，自动取款机 (ATM) 的组件。

背景技术

[0002] 自助服务终端 (SST) 包括向用户出售货物或者为用户提供服务的机器。自助服务终端 (SST) 的一个典型例子是自动取款机 (ATM)。这些机器在某处安装之后，当出现故障或者需要进行维修时，工程师或者维护人员通常需要到现场诊断问题并修复故障。如果修复故障需要安装替换组件，则存在风险，就是替换组件的标准可能低于该自助服务终端 (SST) 的制造商的原装组件。

[0003] 以自动取款机 (ATM) 为例，由于自动取款机 (ATM) 被用作金融交易的界面，所以要对替换组件特别关注，确保其是高标准的。此外，自动取款机 (ATM) 通常是窃贼的目标，例如，为了获得自动取款机 (ATM) 上后来的用户输入的安全信息，怀有恶意的窃贼可能故意在自动取款机 (ATM) 上安装一个替换组件。

[0004] 在一种现有技术的方法中，该问题是这样解决的，即要求工程师在安装好替换组件之后，确认其处在良好的工作状态。该过程实际按下述过程进行：

[0005] 当一个工程师被叫到自助服务终端 (SST) 的故障现场时，他或她就使用自动取款机 (ATM) 内部的称作操作面板的设备。操作面板是一个处理单元，它为工程师提供了一个用户界面，并且引导工程师进行维修和诊断过程。为了执行这些过程，工程师必须通过安全许可测试。这通常是通过要求工程师使用一个在这种环境中公知为服务安全密钥 (Service Security Key) 的 USB 安全软件狗来实现的。

[0006] 在维修自助服务终端 (SST) 时，工程师可能需要替换一个故障组件。设置自助服务终端 (SST)，使得在其恢复正常运行状态之前，需要验证该组件能够完全正常工作。这种方法的问题在于，如果工程师没有带自己的服务安全密钥，或者密钥本身发生故障，那么该自助服务终端 (SST) 将无法恢复到正常操作状态。而且，即使该方法确保了替换组件正常工作，但是并不确保该替换组件来自受信任的来源。

发明内容

[0007] 根据本发明的第一方面，提供一种验证自助服务终端 (SST) 中的机器组件的方法，包括：提供至少一个带有机器可读标识符形式的标识信息的机器组件；从所述机器可读标识符中读取标识数据；将所述标识数据与所存储的标识数据进行比较，以确定组件的标识是否已改变；如果所述标识已改变，比较所述标识数据和来源数据以确定该组件来自受信任的来源。

[0008] 这提供了一个检验组件的质量和完整性的便利方法。可以理解，自助服务终端 (SST) 经常接收现金，而有些 SST，例如自动取款机 (ATM)，被用于金融交易。这意味着终端

的组件必须保持高标准。如果组件来自受信任的来源，则可假设这种高标准将被满足。此外，由于终端经常会成为坏人的目标，所以，能够验证组件是真的并且不能被用于欺骗终端用户是非常重要的。

[0009] 该方法优选地在终端启动时执行。由于为了替换组件终端设备通常会被关闭，所以这是合宜的。在启动时检查任何替换组件的来源意味着在使用终端之前就能够发现任何来自非受信任来源的组件。

[0010] 在这样一种实施例中，该方法可以包括：如果组件不是来自受信任的来源，就禁止使用终端。这是有益的，因为它避免了装有不受信任的组件的终端的运行。

[0011] 该方法还包括：如果标识已改变，就使用已改变的标识替换所存储的标识。这是有益的，因为在未来替换组件之前，该组件的来源将不会被确定。

[0012] 在优选实施例中，该方法包括：在使用已改变的标识数据替换所存储的标识数据之前，验证安全数据。这是有益的，因为这有助于确保任何组件的替换都是由经过授权的操作人员或者工程师完成的。

[0013] 根据本发明的第二方面，提供一种自助服务终端（SST）的处理单元，包括：存储标识数据的存储器，用于向终端的组件请求标识数据的请求装置，以及用于将请求装置收到的标识数据与所存储的标识数据进行比较以发现标识数据的任何改变的比较装置。

[0014] 在一个实施例中，所述处理单元的存储器包括组件来源数据，并且安排所述比较装置对改变的标识数据和所述来源数据进行比较，以确定该组件是否来自受信任的来源。

[0015] 处理单元优选地还包括一个安全装置，用来接收来自维护操作人员的安全数据并且使用该安全数据来确定维护操作人员是否是经过授权的操作人员。

[0016] 优选地，安排所述处理单元，使得仅当所述组件或每个组件来自受信任的来源，才允许与其相关联的终端运行。

[0017] 根据本发明的第三方面，提供一种自助服务终端（SST），包括根据本发明第二方面的处理单元，并且还包括如下组件的至少之一：加密个人识别号（PIN）键盘、现金给付单元和读卡器，并且安排所述终端，使得与该组件或每个组件相关联的识别数据可被所述处理单元读取。

[0018] 在优选实施例中，所述终端包括上述每种组件中的一个，并且所述处理单元被安排用于确定每个组件是否来自受信任的来源，并且只有在所有组件都来自受信任的来源时才允许终端运行。

[0019] 优选地，与该组件或每个组件相关联的标识数据被设置在芯片上。

[0020] 在一个实施例中，所述自助服务终端（SST）是自动取款机（ATM）。

[0021] 根据本发明的第四方面，提供用来执行本发明的第一方面的方法的计算机软件。

[0022] 根据本发明的第五方面，提供在将其加载到处理单元上时使处理单元充当本发明的第二方面的处理单元的计算机软件。

[0023] 本发明的上述和其它目标、特性及优势将在下面的描述和附图中得到明显体现。

附图说明

[0024] 图 1 示出了一个自助服务终端（SST）的外观。

[0025] 图 2 示意性示出了根据本发明的一个实施例的自助服务终端（SST）的内部的组

件。

[0026] 图 3 示出了自动取款机 (ATM) 在“首次”启动时的步骤的流程图。

[0027] 图 4 示出了自动取款机 (ATM) 在后续启动中的步骤的流程图。

具体实施方式

[0028] 图 1 和图 2 所示的自助服务终端 (SST) 是自动取款机 (ATM) 100。ATM 100 包括屏幕 102、插卡槽 104、16 键的键盘 106 形式的数据输入设备和菜单选择按钮 108、以及给付槽 110。

[0029] 图 2 示出了 ATM 100 的组件。组件包括加密个人识别号 (PIN) 键盘 202、现金给付单元 204 和读卡器 206。ATM 100 还包括 PC 内核 208 形式的处理单元。每一个组件包括嵌在其中的包括提供了制造商标识的数据的标识芯片 212。加密个人识别号键盘 202、现金给付单元 204、读卡器 206 以及与组件 202、204 和 206 相关联的芯片 212 能够通过系统总线 210 与 PC 内核 208 进行通信。

[0030] PC 内核 208 包括用来存储数据的存储器 214。存储器 214 能够存储持久化数据，即，以非易失的方式存储数据。PC 内核 208 还包括用来向芯片 212 请求和接收数据的请求装置 216，以及用来把请求装置接收的标识数据和存储在存储器 214 中的标识数据进行比较的比较装置 218。PC 内核 208 还包括安全装置 220，用来执行对维护操作人员或者工程师进行身份验证的安全例程，以确保该人有权安装替换组件 202、204 和 206。

[0031] 在正常使用 ATM 100 时，用户将带有磁条和 / 或加密数据芯片的卡（通常是银行卡）插入插卡槽 104。读卡器 206 读取磁条或者加密数据芯片以获得与该卡相关联的细节，包括加密的个人识别码 (PIN) 数据。接着屏幕 102 被用来显示要求用户输入 PIN 的消息，用户则使用键盘 106 输入该 PIN。将输入的数据提交给加密 PIN 键盘 202，该加密 PIN 键盘对所输入的数字进行加密。将加密的结果与从卡中读取的加密 PIN 数据进行比较，假设两者相匹配，那么用户可以通过使用菜单选择按钮 108 选择屏幕 102 上显示的服务来使用 ATM 100 的服务。如果用户要提取现金，现金给付单元 204 将从提供不同面值的一系列现金堆中选出所需的纸币，并将现金传送到给付槽 110，用户就可以在此提取现金。

[0032] 现在描述 ATM 100 的另外两个启动实例。参考图 3 所示的流程图描述了 ATM 100 “首次”启动的过程。然后参考图 4 所示的流程图描述了后续每一次启动中的对组件的验证过程。

[0033] 在“首次”启动之前，ATM 100 由已知来源的组件组成，包括加密 PIN 键盘 202，现金给付单元 204，读卡器 206 和 PC 内核 208（步骤 302）。在该环境中，“已知来源”可以是指组件 202、204、206 的制造商是已知的，并已被确定为高质量的、可靠的组件 202、204、206 的受信任的来源。PC 内核 208 的请求装置 216 通过系统总线 120 向组件 202、204、206 请求制造商的标识数据（步骤 304）。在步骤 306，组件 202、204、206 分别提供所需数据，在本例中，该数据包括序列号。在步骤 306，该数据作为持久化数据被保存在 PC 内核 208 的存储器 214 中。

[0034] 在每一次后续启动中（步骤 402），PC 内核 208 的请求装置 216 再次通过系统总线 120 向组件 202、204、206 请求制造商的标识数据（步骤 404）。在步骤 406，组件 202、204、206 中的每一个将所需数据提供给请求装置 216。在步骤 408，PC 内核 208 的比较装置 218

将所提供的每一个标识对照所存储的标识进行核对。如果所有标识数据都没有任何变化，那么 ATM 的启动过程就在步骤 409 结束。如果某一个或多个组件的标识发生了变化，那么在步骤 410，PC 内核 208 的比较装置 218 就检查新组件是否来自受信任的来源。

[0035] 在该实施例中，来自已知来源的组件的标识是序列号的形式，该序列号与可被处理以验证其身份的预定格式一致。然而，在其他实施例中，PC 内核 208 可对照存储在数据库中的标识来验证该标识，而该数据库可能是远离 ATM 100 的。

[0036] 如果新组件 202、204、206 并非来自受信任的来源，那么在步骤 412 禁用 ATM 100。然而，如果新组件确实来自受信任的来源，那么 PC 内核 208 要求工程师输入安全数据以确保新组件的安装是由经过授权的人员完成的（步骤 414）。在本例中，通过在该环境中公知被称为服务安全密钥的 USB 安全软件狗的方式提供安全数据。

[0037] 在步骤 416，PC 内核 208 的安全装置 220 检查服务安全密钥是否属于被授权的工程师。如果并非如此，那么在步骤 418，ATM 100 被禁用。如果工程师是被授权的，那么在步骤 420，PC 内核使用新的标识数据更新其存储器 214。然后，就在步骤 422 结束 ATM 100 的启动过程。

[0038] 可以理解，只是通过举例的方式给出了优选实施例的上述描述，本领域的普通技术人员可以做出各种修改。例如，芯片 212 可能被射频识别（RFID）标签或诸如可采用蓝牙或者红外技术读取的其它的可远程访问的数据存储装置所代替。由于这些装置可以远程读取，所以不再需要系统总线 214。

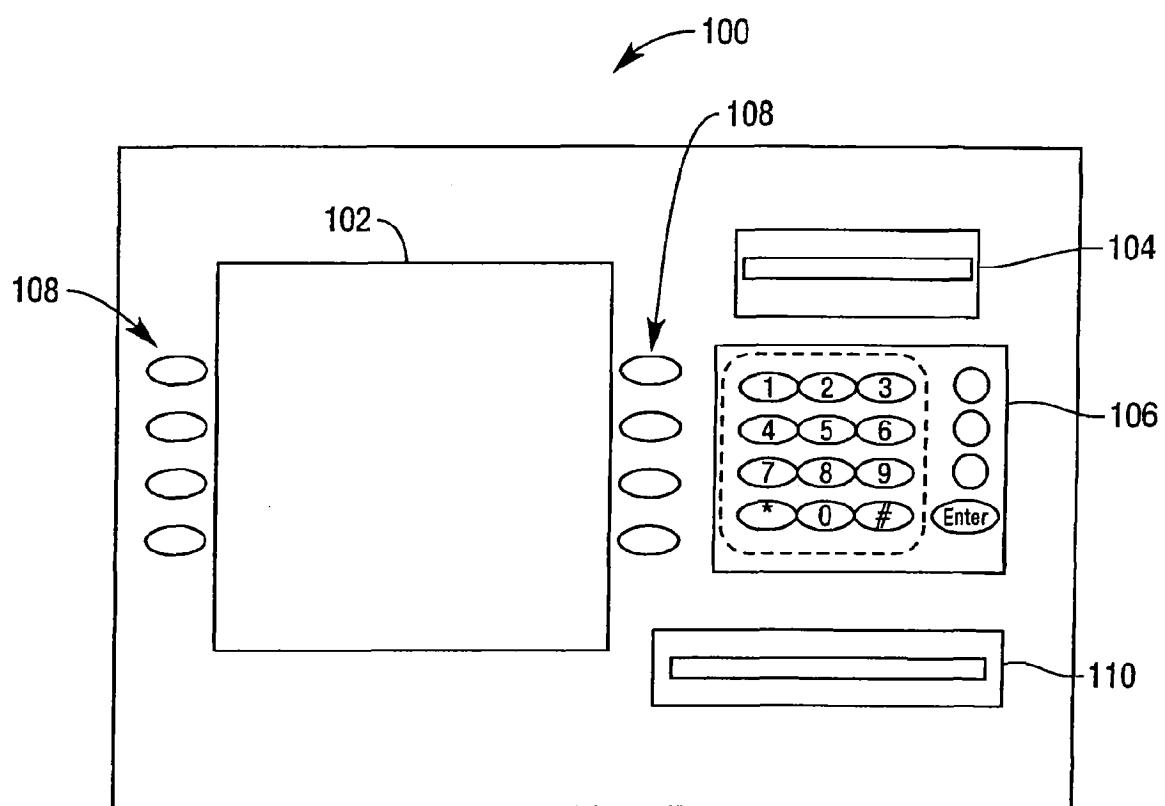


图1

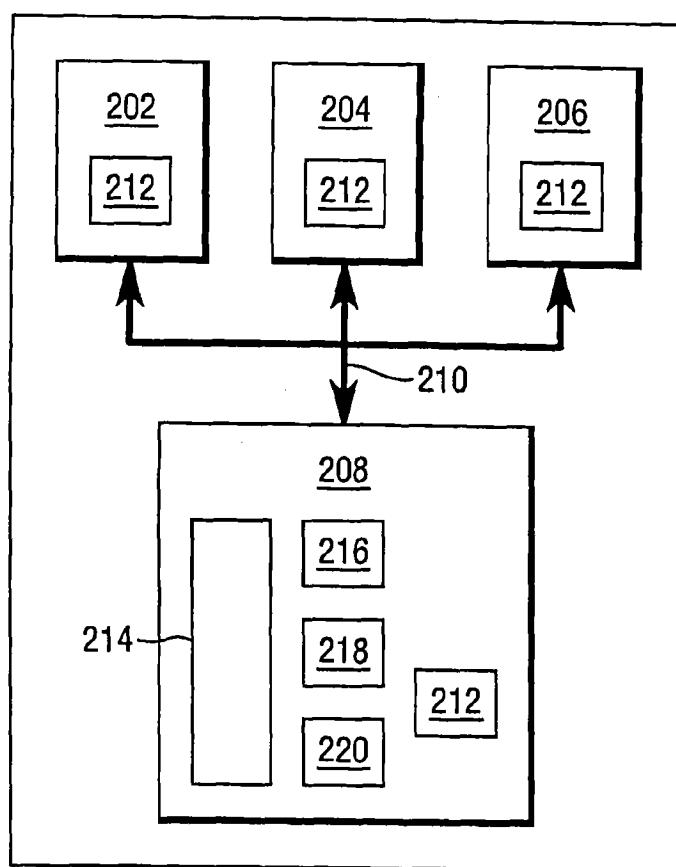


图2

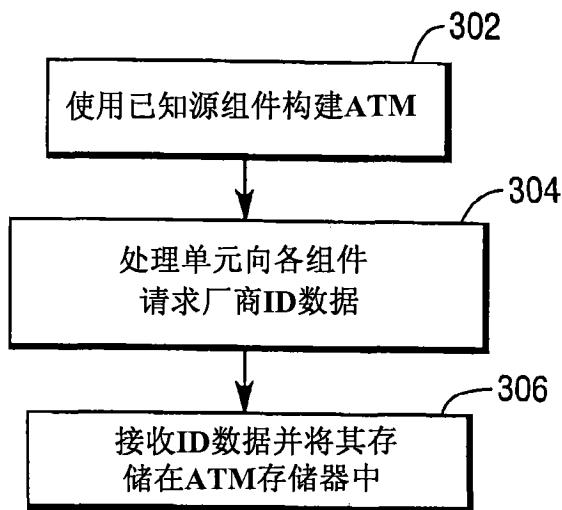


图3

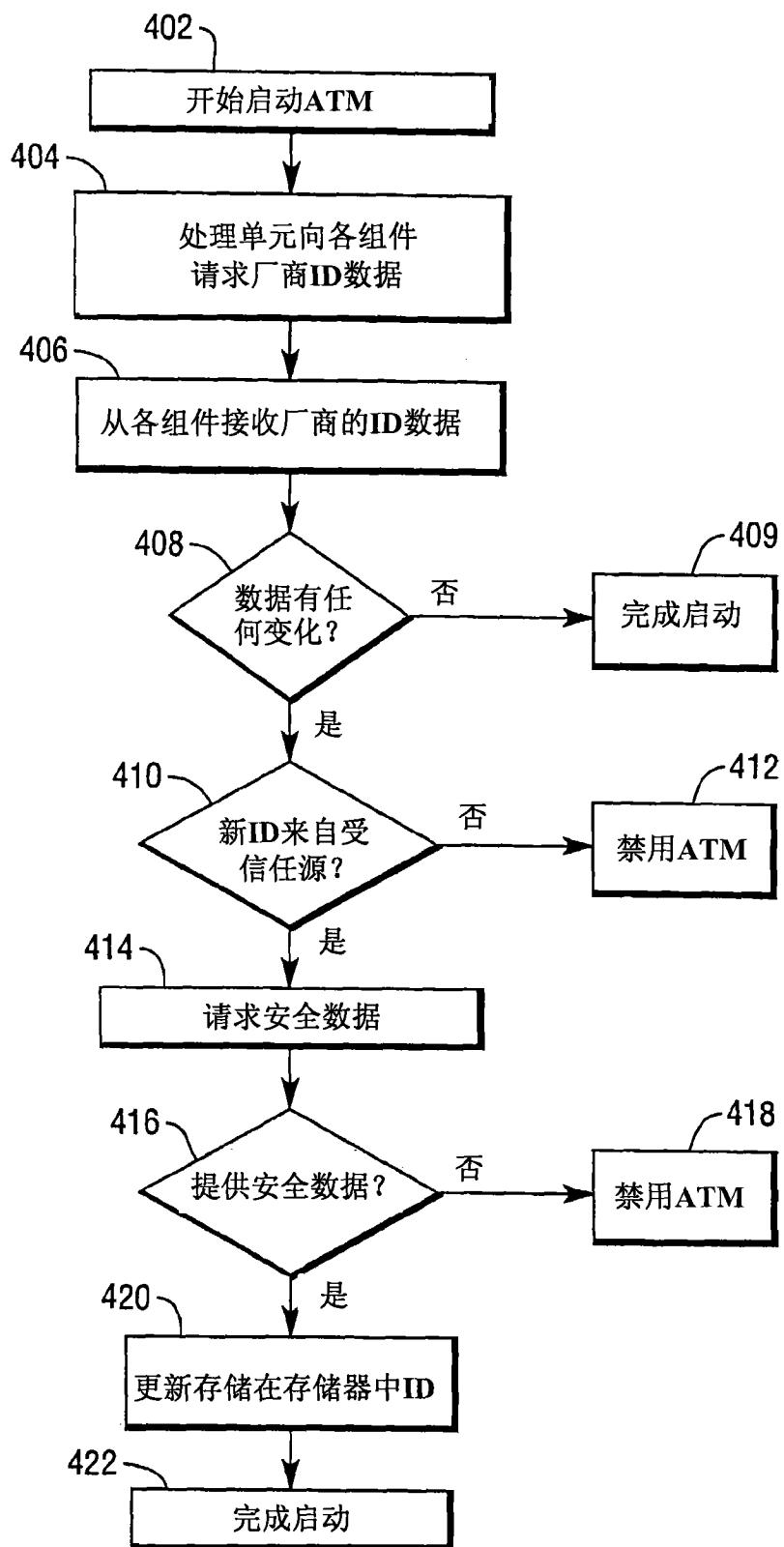


图4