



(19) **United States**

(12) **Patent Application Publication**
Bahr

(10) **Pub. No.: US 2005/0138169 A1**

(43) **Pub. Date:** **Jun. 23, 2005**

(54) MANAGEMENT OF WORKSPACE DEVICES

Publication Classification

(76) Inventor: **Casey Bahr**, Hillsboro, OR (US)

(51) **Int. Cl.⁷** **G06F 15/173**; G06F 11/30

(52) **U.S. Cl.** **709/224; 713/201**

Correspondence Address:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN

12400 WILSHIRE BOULEVARD

SEVENTH FLOOR

LOS ANGELES, CA 90025-1030 (US)

(57)

ABSTRACT

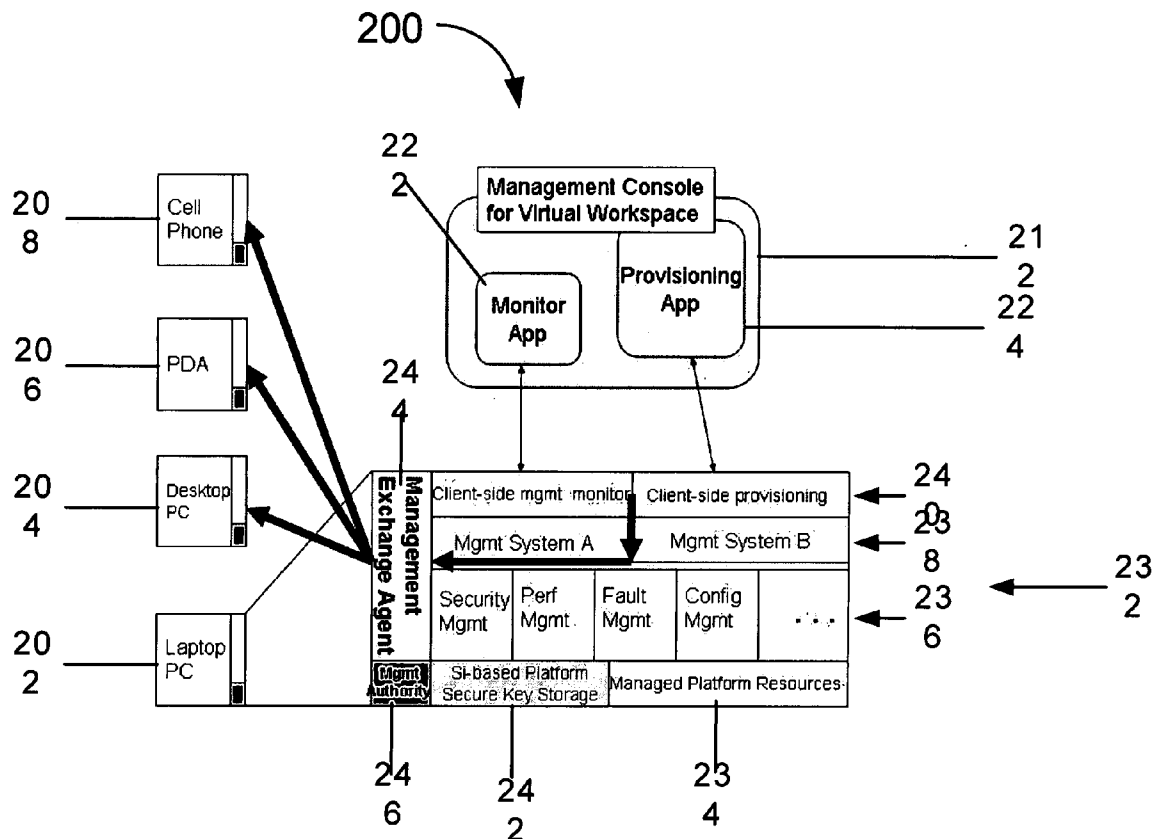
(21) Appl. No.: **11/026,608**

(22) Filed: **Dec. 30, 2004**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/742,225, filed on Dec. 18, 2003.

In some embodiments, management operations are received from a management console at a first device of a plurality of devices to be used by a user, and management authority and operations are performed on a second device of the plurality of devices in response to the received management operations. Other embodiments are described and claimed.



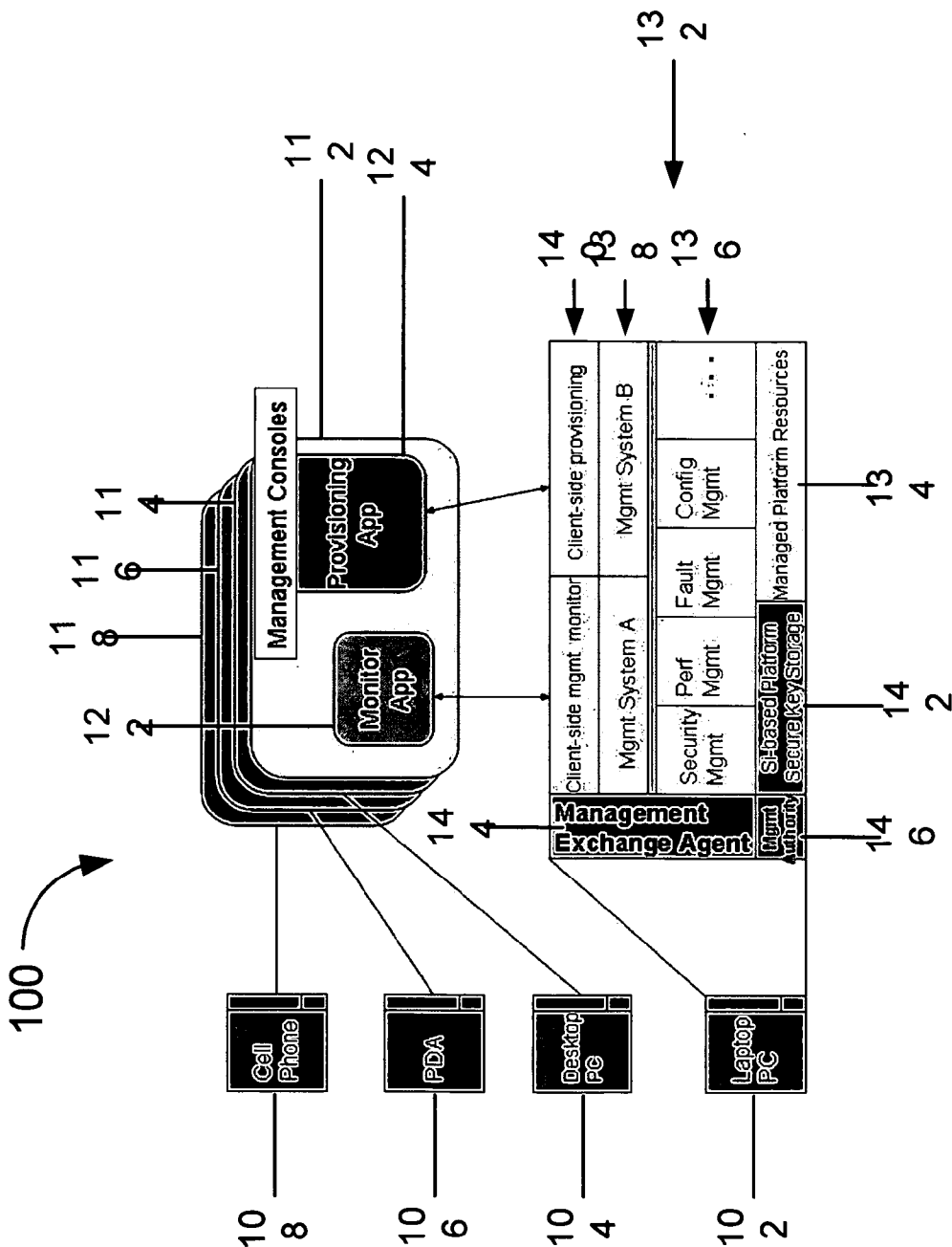


FIG 1

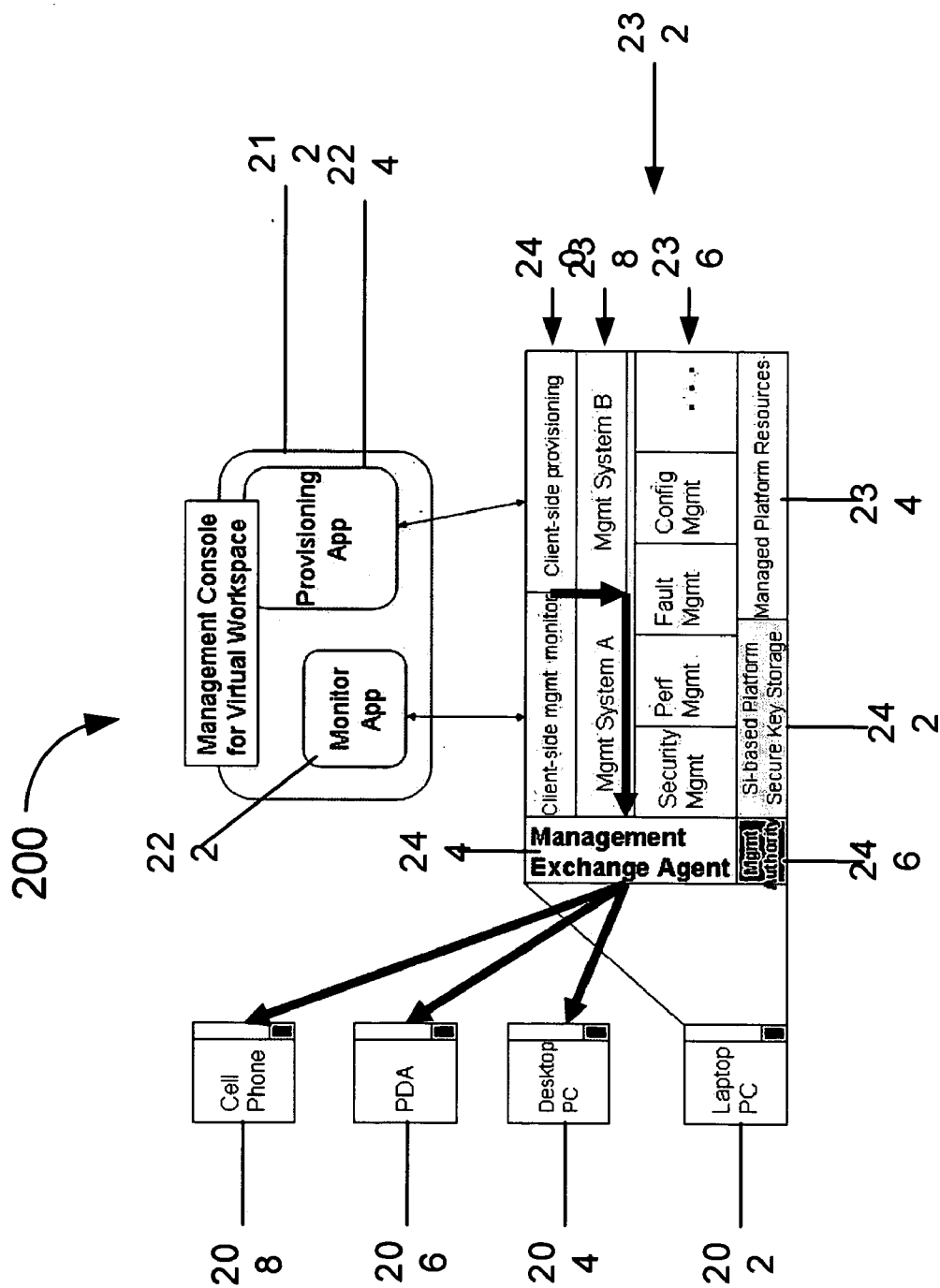


FIG 2

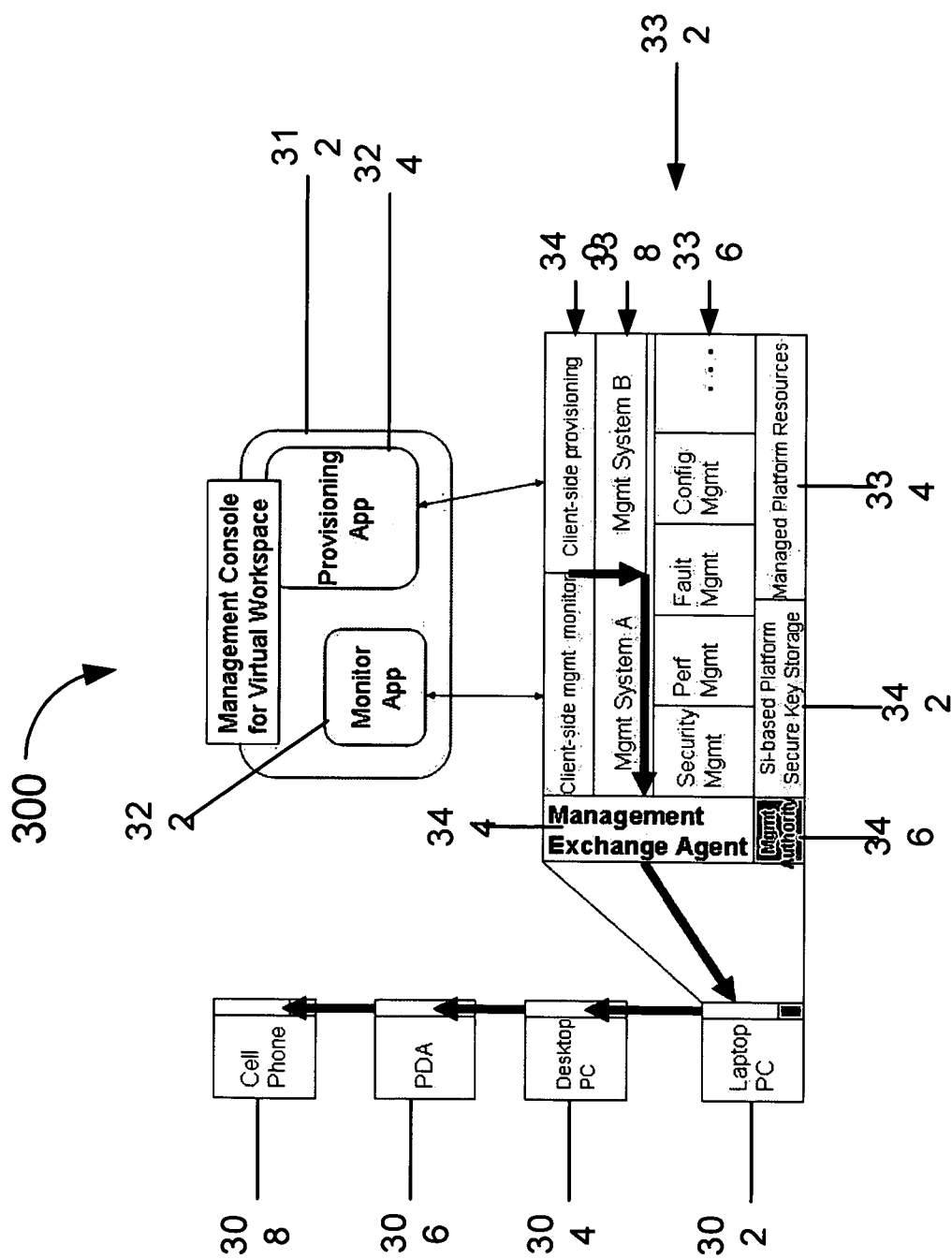


FIG 3

MANAGEMENT OF WORKSPACE DEVICES

[0001] This application is a Continuation-In-Part application of U.S. patent application Ser. No. 10/742,225 filed on Dec. 18, 2003 and entitled "Client-Side Security Management for an Operations, Administration, and Maintenance System for Wireless Clients" by Casey Bahr.

TECHNICAL FIELD

[0002] The inventions relate to management of workspace devices.

BACKGROUND

[0003] Information Technology (IT) departments typically manage an employee's collection of enterprise-provisioned devices such as a laptop, a desktop, a PDA (personal digital assistant), a smart cell phone, etc. separately from each other. Enterprise IT departments currently struggle to achieve the best cost and performance solution.

[0004] Several long-term and emerging trends in computer and communication technologies promise continued increases in worker productivity. For example, these trends include an increasing sophistication of the computers or devices themselves, multiple devices of varying computation and communication capabilities for each enterprise worker (since a worker distributes their work over these devices in the most optimal manner for the context or task in which they are working in order to create a "virtual workspace"), and/or flexibility due to an extension in an employee's work time and space which may include multiple work locations such as roaming the enterprise, telecommuting from home, traveling, etc.

[0005] These types of trends have created new challenges for IT departments that are charged with managing these devices (for example, provisioning, configuration, monitoring, tuning, securing, etc.) For example, the devices may not be equipped with effective management infrastructure or tools. Further, if such infrastructure exists it may vary in functionality from platform to platform or from vendor tool to vendor tool. Another challenge includes the diversity of network connectivity options, both public and private. For example, a device may connect to a network using one or more of the following or any other available connectivity options: Wireless Local Area Networks (WLANs) (for example, 802.11x hotspots), Wireless Wide Area Networks (WWANs) (for example, General Packet Radio Service (GPRS) or Universal Traffic Management Systems (UTMS)), and Personal Area Networks (PANs) (for example, Bluetooth). Such challenges come at a time when IT departments are under continuing pressure to reduce their costs to the enterprise as a whole. These factors have created an increased automation of management processes and a commensurate reduction in IT department employee headcount. Thus, enterprise IT departments struggle to achieve the best cost-performance in their services and are under constant pressure to reduce costs to the enterprise, while they must manage more devices and a wider variety of devices as time goes on.

[0006] Multiple worker devices have previously been managed using one management console (or console application) per device with each device managed independently of the others. This approach increases costs to the enterprise as the number and variety of devices increases.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The inventions will be understood more fully from the detailed description given below and from the accompanying drawings of some embodiments of the inventions which, however, should not be taken to limit the inventions to the specific embodiments described, but are for explanation and understanding only.

[0008] FIG. 1 illustrates a platform management system according to some embodiments of the inventions.

[0009] FIG. 2 illustrates a platform management system according to some embodiments of the inventions.

[0010] FIG. 3 illustrates a platform management system according to some embodiments of the inventions.

DETAILED DESCRIPTION

[0011] Some embodiments of the inventions relate to management of workspace devices.

[0012] In some embodiments the inventions enable an enterprise Information Technology (IT) department to distribute the management of an employee's collection of enterprise-provisioned devices (for example, a laptop computer, a desktop computer, a personal digital assistant (PDA), and/or a smart cell phone, etc.) amongst the devices themselves rather than remotely managing each device as a separate entity.

[0013] In some embodiments the productivity for the management of an employee's device collection is increased. In some embodiments intelligent management agents are able to discover and communicate management functions to identical agents on other platforms. In some embodiments interfaces to intelligent management agents are used to enable routing of platform management operations to other devices. In some embodiments management authority is established over managed resources of a platform (for example, the managed resources can include hardware, software, applications, services, etc.) In some embodiments management authority is delegated from one device to another (for example, another device that includes the same management agents). In some embodiments the above-described features and/or other features may be used to distribute management operations over a collection of devices in various ways that suit a configuration context and/or pre-set policies.

[0014] In some embodiments, management operations are received from a management console at a first device of a plurality of devices to be used by a user, and management authority and operations are performed on a second device of the plurality of devices in response to the received management operations.

[0015] In some embodiments an article includes a computer readable medium having instructions thereon which when executed cause a computer to receive management operations from a management console at a first device of a plurality of devices to be used by a user, and to perform management authority and operations on a second device of the plurality of devices in response to the received management operations.

[0016] In some embodiments a user device includes a management agent to receive management operations from

a management console at the user device, and to perform management authority and operations on a second user device in response to the received management operations, wherein the user device and the second user device are included in a plurality of user devices to be used by a user.

[0017] In some embodiments a system includes a management console to provide management operations and a plurality of devices to be used by a user including at least a first device and a second device. The first device includes a first management agent to receive management operations from the management console, and to perform management authority and operations on the second device in response to the received management operations. The second device includes a second management agent to receive management operations from the first management agent.

[0018] FIG. 1 illustrates a platform management system 100 according to some embodiments. Platform management system 100 includes a plurality of managed devices (for example, a worker's device collection or workspace) including laptop personal computer (PC) 102, desktop PC 104, PDA 106, and cell phone 108. The managed devices according to some embodiments can include any combination of these types of devices illustrated in FIG. 1 and/or any other type of devices. For example, laptop 102 and desktop 104 are not limited to PCs (personal computers) and can be any type of laptop and desktop, respectively. Each of the laptop 102, desktop 104, PDA 106, and cell phone 108 has a corresponding management console 112, 114, 116, and 118, respectively (or in some embodiments a corresponding management console application). One management console (or management console application) 112 is illustrated in the front of the other management consoles (or management console applications) 114, 116, and 118 in FIG. 1, it is noted that each management console can be similar and/or identical to each other in some embodiments. In some embodiments one or more of the management consoles 112, 114, 116, and/or 118 includes a monitor application 122 and a provisioning application 124, as illustrated in management console 112 of FIG. 1. In some embodiments each management console 112, 114, 116, and 118 (or management console application) is managed independent of the other management consoles (or management console applications).

[0019] In some embodiments each of the managed devices 102, 104, 106, and 108 includes a managed platform 132. Although a managed platform 132 is illustrated in FIG. 1 as the managed platform of the laptop 102, each of the other managed devices (desktop 104, PDA 106, and/or cell phone 108) can include a similar or identical managed platform.

[0020] In some embodiments managed platform 132 includes managed platform resources 134, management functions 136 supplied on the platform, management services 138 built on the management functions 136, management applications 140, a secure storage area 142, a Management Exchange Agent (MEA) 144, and a Management Authority component (MA) 146. Many of these management system components (for example, the managed platform resources 134, management functions 136, management services 138, and management applications 140) are exemplary and may not be included in all embodiments.

[0021] The managed platform resources 134 are the platform resources themselves (that is, the things to be man-

aged). In some embodiments managed platform resources 134 of a platform such as laptop 102 can include, for example, hardware, software, applications, and/or services, etc.) In some embodiments the management functions 136 are the fundamental (or basic) management functions supplied on the platform, and can include management functions such as Security Management, Performance Management, Fault Management, Configuration Management, and/or other types of management functions, for example, in various embodiments. In some embodiments a management system including Security Management can be implemented as disclosed, for example, in U.S. patent application Ser. No. 10/742,225 filed on Dec. 18, 2003 and entitled "Client-Side Security Management for an Operations, Administration, and Maintenance System for Wireless Clients". One or more management services 138 are built on the management functions 136 which may be supplied by one or more different management software vendors, for example. In some embodiments management services 138 can include, for example, a management system A and a management system B. In some embodiments management services 138 can include a single management system, or some other number of management systems other than that shown in FIG. 1. In some embodiments any particular type of management system may be used as management services 138. In some embodiments the management applications 140 are the management applications themselves, and can include, for example, a monitoring service (or client-side management monitor as illustrated in FIG. 1) and/or a provisioning application (or client-side provisioning as illustrated in FIG. 1).

[0022] In some embodiments secure storage area 142 is a tamper-proof secure storage area into which keys or their hashes can be installed. The secure storage area 142 can be platform or silicon-based. In some embodiments a secure storage area is not necessary and is not used. However, secure storage area 142 is advantageous in some embodiments because it provides a tamper-proof area to store keys or their hashes, for example, to ensure secure or trusted communications between the platform (for example, laptop 102) and other similarly equipped platforms.

[0023] In some embodiments Management Exchange Agent (MEA) 144 is an intelligent (active) MEA which communicates with other MEAs on other similarly equipped platforms (for example, on desktop 104, PDA 106, and/or cell phone 108).

[0024] In some embodiments each MEA 144 includes a Management Authority component (MA) 146. MA 146 represents the level or specific domain of authority that the MEA 144 has to effect management functions on other devices. This authority may be applied as described and/or derived, for example, in U.S. patent application Ser. No. 10/742,225 filed on Dec. 18, 2003 and entitled "Client-Side Security Management for an Operations, Administration, and Maintenance System for Wireless Clients".

[0025] An embodiment on which an MA of a platform-based security management system could be based are included in certain figures and descriptions of the above-mentioned U.S. patent application Ser. No. 10/742,225. In particular, FIG. 5 of application Ser. No. 10/742,225 illustrates the breadth and depth of possible policy control over access to managed resources in a platform. FIGS. 3 and 4

of application Ser. No. 10/742,225 illustrate the mechanisms for exercising such control, and **FIG. 6** of that application demonstrates the mechanisms for establishing initial authority and delegation of such authority. These mechanisms, in some embodiments, may be used by the MA to derive and delegate its own management authority within its own platform and other platforms over which it may exercise management authority as described elsewhere in this application.

[0026] In some embodiments the MA contains the following functionality, some of which may be optional for some embodiments:

[0027] In some embodiments the MA is a “trusted” non-tamperable set of computer instructions. These instructions may be authenticated and authorized by means of a verifiable certificate or other keys or hashes of keys that are stored on the platform in secure storage area **142**, for example.

[0028] In some embodiments the MA has the ability to present on demand such certification of its authority.

[0029] In some embodiments the MA has the ability to store a non-tamperable representation of any additional authority granted it (e.g. by a Management Console or another MEA). In some embodiments such representation or a certificate of authenticity can be stored in secure storage area **142**.

[0030] In some embodiments the MA has the ability to retrieve and process authority representations (e.g. certificates) from a Management Console or other MEA with which its MEA communicates. It should have the ability to accomplish this independent of verification from a 3rd party such as a 2nd Management Console or another MEA.

[0031] In some embodiments the MA must understand the representation of the security policy being applied ultimately from the Management Console. For example, in some embodiments, management authority may be restricted to read-only access or read-write access and only for particular management operations or particular management resources including entire platforms. Thus, the MA must know how to apply the security policy to other platforms as well as the resources within its own platform. The infrastructure for such policies could be provided by the aforementioned mechanisms with the patent application Ser. No. 10/742,225.

[0032] In some embodiments the MEA **144** and/or the MA **146** provide a way to increase the productivity for managing an employee’s device collection using the following features:

[0033] 1. Intelligent management agents that are able to discover and communicate management functions to identical agents on other platforms.

[0034] 2. Interfaces to such management agents through which platform management operations can be routed to other devices.

[0035] 3. Establishing management authority over a platform managed resource (for example, hardware, software, applications, services, etc.)

[0036] 4. Delegating the management authority from one device to another device (which has the same or similar features, functionality, mechanisms, etc.)

[0037] 5. Utilizing the above features to distribute management operations over a collection of devices in various ways that suit a configuration context or pre-set policies.

[0038] In some embodiments a Management Exchange Agent (for example MEA **144** of **FIG. 1** or any other MEA) may communicate with one or two other entities:

[0039] 1. The Management Console from which it may take initial instructions and to which it may provide acknowledgment of actions taken on behalf of the Console.

[0040] 2. Another MEA to which the first MEA must transmit management instructions and optionally from which it must receive acknowledgment of the management actions requested by the first MEA.

[0041] In some embodiments a particular MEA may participate in either one or both of these communications depending on the role of its platform in executing management instructions. For instance:

[0042] The platform on which the MEA resides may be the only platform which the Console wishes to manage, in which case only communication 1. applies

[0043] The platform may be the first of a plurality of platforms that the Console wishes to manage by means of the inventions and thus the MEA will utilize both forms of communication above, 1. and 2.

[0044] The platform may be under the ultimate management of the Console, but not directly. In this case, this platform’s MEA will communicate with another MEA whether it be the first or an intermediate MEA in a chain of management delegation.

[0045] In some embodiments an MEA (for example, MEA **144** of **FIG. 1** or any other MEA) will have the following functionalities:

[0046] 1. The presentation of initial or subsequent interfaces to a requesting entity (i.e. the Management Console or another MEA).

[0047] 2. Authentication of itself to a Console or another MEA for the purposes of establishing a trusted relationship and secure communication with the requesting entity.

[0048] 3. The acceptance of a set of management instructions and policies related to the use of these instructions.

[0049] 4. The application of the management instructions and policies. This feature means that management functionality exists to at least the extent that the instructions and policies can be applied within the MEA. This set of management functionality may be less than that offered by the “Management Systems” depicted in **FIG. 1**, since it need not be general-purpose.

[0050] 5. The ability to retain state related to the management instructions being applied such that the instructions can be applied transactionally (or atomically) to support roll-back of the instructions in case of errors.

[0051] 6. The ability to retain acknowledgment state that is required to be communicated back up an MEA chain, ultimately to the Console.

[0052] 7. Notification back up an MEA chain to a Console for the purposes of acknowledgement of a set of management functions (including errors).

[0053] In some embodiments only functionalities 3 and 4 are strictly required, and the other functionalities are optional (though likely to be present in some embodiments). Other functionalities may be present in some embodiments.

[0054] In some embodiments the kind of data included in the MEA management instruction policy may include some or all of the following:

[0055] Various time markings to show when the management instructions were issued, their deadline for delivery, or a deadline for acknowledgment.

[0056] What level of security or trust must be utilized when communicating and applying the management instructions

[0057] What, if any, interaction is required from the owner or user of the platform being managed

[0058] What sorts of transport are acceptable for communicating the management instructions from one platform to another

[0059] What, if any, other software or hardware must be or must not be present before applying the management instructions (e.g. if previously installed supporting management software is to be utilized)

[0060] What, if any, acknowledgement is required back to the transmitting MEA or Console

[0061] In the case of errors, what actions to take, perhaps to the level of specific errors (e.g., roll-back, abort, warning, etc.).

[0062] FIG. 2 illustrates a platform management system 200 according to some embodiments. In some embodiments FIG. 2 illustrates a distribution of management operations from a single management console via one device, which exerts management authority and operations over other devices in the collection of devices. Platform management system 200 includes a plurality of managed devices (for example, a worker's device collection) including laptop 202, desktop 204, PDA 206, and cell phone 208. The managed devices according to some embodiments can include any combination of these types of devices illustrated in FIG. 2 and/or any other type of devices. Platform management system 200 also includes a management console (or management console application) 212 for the managed devices 202, 204, 206, and 208. Management console 212 includes a monitor application 222 and a provisioning application 224. In some embodiments each of the managed devices 102, 104, 106, and 108 includes a managed platform 232. Although a managed platform 232 is illustrated in detail in FIG. 2 as the managed platform of the laptop 202, each of the other managed devices (desktop 204, PDA 206, and/or cell phone 208) can include a similar or identical managed platform.

[0063] In some embodiments managed platform 232 includes managed platform resources 234, management functions 236, management services 238, management applications 240, a secure storage area 242, a Management Exchange Agent (MEA) 244, and a Management Authority component (MA) 246. These elements of managed platform 232 can be similar to or the same as similar elements of managed platform 132 of FIG. 1.

[0064] FIG. 2 illustrates some embodiments in which the MEA 244 and MA 246 components may be utilized. In some embodiments laptop 202 has been granted management authority over all of the other devices (for example desktop 204, PDA 206, and/or cell phone 208) in the worker's collection of devices.

[0065] As illustrated by arrows in FIG. 2, for example, an enterprise IT craftsman may wish to apply a management function to the collection of devices as a whole (for example, an asset information update, a security patch, etc.) As each device is contacted by the laptop MEA 244 via its own MEA within that other device, management authority is granted on a per device basis, as illustrated by the arrows. This is accomplished, for example, by an exchange of MA keys derived from the secure platform storage area 242. Management operations are routed through the MEA 244 to each device individually. In some embodiments all the devices do not need to be present or connected at the same time for the management operations to take place. The laptop MEA 244 may apply the operations at any time the laptop 202 comes into contact with the other devices (for example, via Bluetooth, 802.11x, Universal Serial Bus, and/or any other way). In some embodiments the MEA 244 also has a reporting function (not illustrated by arrows in FIG. 2) used to report back to the management console the status of any operations.

[0066] FIG. 3 illustrates a platform management system 300 according to some embodiments. In some embodiments FIG. 3 illustrates a management of a virtual workspace in which each device individually exerts management authority and operations over the next device in the collection of devices. In some embodiments this management operation exchange can occur asynchronously as devices are available. Platform management system 300 includes a plurality of managed devices (for example, a worker's device collection) including laptop 302, desktop 304, PDA 306, and cell phone 308. The managed devices according to some embodiments can include any combination of these types of devices illustrated in FIG. 3 and/or any other type of devices. Platform management system 300 also includes a management console (or management console application) 312 for the managed devices 302, 304, 306, and 308. Management console 312 includes a monitor application 322 and a provisioning application 324. In some embodiments each of the managed devices 302, 304, 306, and 308 includes a managed platform 332. Although a managed platform 332 is illustrated in detail in FIG. 2 as the managed platform of the laptop 302, each of the other managed devices (desktop 304, PDA 306, and/or cell phone 308) can include a similar or identical managed platform.

[0067] In some embodiments managed platform 332 includes managed platform resources 334, management functions 336, management services 338, management applications 340, a secure storage area 342, a Management Exchange Agent (MEA) 344, and a Management Authority component (MA) 346. These elements of managed platform 332 can be similar to or the same as similar elements of managed platform 132 of FIG. 1 and/or of managed platform 232 of FIG. 2.

[0068] FIG. 3 illustrates a management operation distribution according to some embodiments and as illustrated by the arrows in FIG. 3. For example, in some embodiments

the laptop MEA **344** contacts one of the other devices (for example, desktop **304**) and passes both the management authority and management operations to that device. That device in turn performs the management operations to one of the other devices (for example, PDA **306**) in a similar fashion, and passes on the management authority and management operations to that device to further propagate the operations for all devices in the worker's virtual workspace (for example, the PDA **306** then performs the management operations to cell phone **308** in a similar fashion, and passes on the management operations and/or management authority to that device). In some embodiments a reporting function (not illustrated by arrows in **FIG. 3**) propagates back through the chain of devices to the management console **312** to report status.

[0069] In some embodiments other implementations are performed that mix the functions illustrated in **FIG. 1**, **FIG. 2**, and/or **FIG. 3**, for example. In some embodiments management operations are distributed with a maximum amount of flexibility.

[0070] In some embodiments (such as illustrated in and described in reference to **FIGS. 2 and 3**) a single management console (**212** or **312**, for example) is used rather than multiple management consoles (**112**, **114**, **116**, **118**, for example). In embodiments in which a single management console (or console application) is used a reduction in management overhead is achieved for example, for a console operator to check one console in needing to manage and track each device of a worker.

[0071] In some embodiments a Management Console delegates its authority to an MA of a user's (or worker's) device. In some embodiments an MA of a first user (or worker) device delegates its authority (which authority was derived from a Management Console) to an MA of a second user (or worker) device. These types of delegation relieve the Console of the burden of having to manage each device and/or platform separately. In some embodiments authority is delegated by a management console to a first device to perform management operations on the behalf of the management console on one or more of the plurality of devices in the user's workspace.

[0072] As discussed above, enterprise IT departments currently struggle to achieve the best cost-performance in their services and are under constant pressure to reduce costs to the enterprise, even though they must manage a wider number and variety of devices as time moves forward. One alternative would be to resist integration of multiple and various devices and risk impact to business processes and worker productivity or "black market" management by the workers themselves in a non-uniform manner. One of the barriers that must be overcome is the inability to delegate management authority and operations to systems that can perform these functions automatically with only minimal high-level guidance. In some embodiments such automation is accomplished by distributing console intelligence and authority amongst the devices to be managed.

[0073] In some embodiments the number of consoles (or management applications) required to manage a collection of devices is reduced. This allows for a reduction in the ratio of IT resources to number of devices.

[0074] In some embodiments the number of console operations or the time to apply them may be reduced, since they are applied to other devices automatically.

[0075] In some embodiments collaborative, cross-device applications can be managed as a single entity, since distributed commands or operations are provided from a single point of control.

[0076] In some embodiments management operations (for example, a virus patch) may be applied in a scalable fashion, since only a single point of contact is necessary from IT to the multiple devices held by a single worker.

[0077] In some embodiments enterprise security may be enhanced by using the ability to quarantine an entire device collection from a single point (for example, assuming all devices in a worker's collection or virtual workspace are infected if one device is infected).

[0078] In some embodiments backup and restore operations may be distributed within a collection of devices.

[0079] In some embodiments remote control is implemented of devices from a management console or another device in the collection using another device in the collection as a proxy.

[0080] In some embodiments IT budgets may be reduced by utilizing management automation. In some embodiments built-in security features are incorporated into a platform. In some embodiments multiple devices include built-in security features. In some embodiments all devices in a network or a collection of a worker's devices include management authority and management operations functionality.

[0081] In some embodiments enterprise management is implemented with an ability to perform collaborative, cross-device management of the devices, and the management applications are implemented via intelligent management agents with platform-based management authority.

[0082] Although some embodiments have been described in reference to particular implementations, other implementations are possible according to some embodiments. Additionally, the arrangement and/or order of circuit elements or other features illustrated in the drawings and/or described herein need not be arranged in the particular way illustrated and described. Many other arrangements are possible according to some embodiments.

[0083] In each system shown in a figure, the elements in some cases may each have a same reference number or a different reference number to suggest that the elements represented could be different and/or similar. However, an element may be flexible enough to have different implementations and work with some or all of the systems shown or described herein. The various elements shown in the figures may be the same or different. Which one is referred to as a first element and which is called a second element is arbitrary.

[0084] In the description and claims, the terms "coupled" and "connected," along with their derivatives, may be used. It should be understood that these terms are not intended as synonyms for each other. Rather, in particular embodiments, "connected" may be used to indicate that two or more elements are in direct physical or electrical contact with each other. "Coupled" may mean that two or more elements are in direct physical or electrical contact. However, "coupled" may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

[0085] An algorithm is here, and generally, considered to be a self-consistent sequence of acts or operations leading to a desired result. These include physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be understood, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0086] Some embodiments may be implemented in one or a combination of hardware, firmware, and software. Some embodiments may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by a computing platform to perform the operations described herein. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, the interfaces that transmit and/or receive signals, etc.), and others.

[0087] An embodiment is an implementation or example of the inventions. Reference in the specification to “an embodiment,” “one embodiment,” “some embodiments,” or “other embodiments” means that a particular feature, structure, or characteristic described in connection with the embodiments is included in at least some embodiments, but not necessarily all embodiments, of the inventions. The various appearances “an embodiment,” “one embodiment,” or “some embodiments” are not necessarily all referring to the same embodiments.

[0088] If the specification states a component, feature, structure, or characteristic “may,” “might,” “can” or “could” be included, for example, that particular component, feature, structure, or characteristic is not required to be included. If the specification or claim refers to “a” or “an” element, that does not mean there is only one of the element. If the specification or claims refer to “an additional” element, that does not preclude there being more than one of the additional element.

[0089] Although flow diagrams and/or state diagrams may have been used herein to describe embodiments, the inventions are not limited to those diagrams or to corresponding descriptions herein. For example, flow need not move through each illustrated box or state, or in exactly the same order as illustrated and described herein.

[0090] The inventions are not restricted to the particular details listed herein. Indeed, those skilled in the art having the benefit of this disclosure will appreciate that many other variations from the foregoing description and drawings may be made within the scope of the present inventions. Accordingly, it is the following claims including any amendments thereto that define the scope of the inventions.

What is claimed is:

1. A method comprising:

receiving management operations from a management console at a first device of a plurality of devices to be used by a user; and

performing management authority and operations on a second device of the plurality of devices in response to the received management operations.

2. The method of claim 1, further comprising reporting back to the management console a status of management operations.

3. The method of claim 1, wherein the plurality of devices to be used by a user include at least one of a laptop computer, a desktop computer, a personal digital assistant, or a cell phone.

4. The method of claim 1, wherein the management authority is a management authority over platform managed resources.

5. The method of claim 4, wherein the platform managed resources include at least one of hardware, software, applications, or services.

6. The method of claim 1, further comprising performing the management authority and operations in response to a stored key.

7. The method of claim 1, wherein the plurality of devices is a collection of devices to be used by an employee.

8. The method of claim 1, further comprising delegating authority from the management console to the first device to perform management operations on behalf of the management console on one or more other of the plurality of devices to be used by the user.

9. An article comprising:

a computer readable medium having instructions thereon which when executed cause a computer to:

receive management operations from a management console at a first device of a plurality of devices to be used by a user; and

perform management authority and operations on a second device of the plurality of devices in response to the received management operations.

10. The article of claim 9, the computer readable medium further having instructions thereon which when executed cause a computer to report back to the management console a status of management operations.

11. The article of claim 9, wherein the plurality of devices to be used by a user include at least one of a laptop computer, a desktop computer, a personal digital assistant, or a cell phone.

12. The article of claim 9, wherein the management authority is a management authority over platform managed resources.

13. The article of claim 12, wherein the platform managed resources include at least one of hardware, software, applications, or services.

14. The article of claim 9, the computer readable medium further having instructions thereon which when executed cause a computer to perform the management authority and operations in response to a stored key.

15. The article of claim 9, wherein the plurality of devices is a collection of devices to be used by an employee.

16. The article of claim 9, the computer readable medium further having instructions thereon which when executed

cause a computer to delegate authority from the management console to the first device to perform management operations on behalf of the management console on one or more other of the plurality of devices to be used by the user.

17. A user device comprising:

a management agent to receive management operations from a management console at the user device, and to perform management authority and operations on a second user device in response to the received management operations, wherein the user device and the second user device are included in a plurality of user devices to be used by a user.

18. The user device of claim 17, the management agent to report back to the management console a status of management operations.

19. The user device of claim 17, wherein the plurality of devices to be used by a user include at least one of a laptop computer, a desktop computer, a personal digital assistant, or a cell phone.

20. The user device of claim 17, wherein the management authority is a management authority over platform managed resources.

21. The user device of claim 20, wherein the platform managed resources include at least one of hardware, software, applications, or services.

22. The user device of claim 17, further comprising a secure storage area to store a key, wherein the management agent is to perform the management authority and operations in response to the stored key.

23. The user device of claim 17, wherein the plurality of devices is a collection of devices to be used by an employee.

24. The user device of claim 17, wherein the management agent is to receive authority delegated from the management console to the user device to perform management operations on behalf of the management console on one or more other of the plurality of devices to be used by the user.

25. A system comprising:

a management console to provide management operations;

a plurality of devices to be used by a user including at least a first device and a second device;

wherein the first device includes a first management agent to receive management operations from the manage-

ment console, and to perform management authority and operations on the second device in response to the received management operations; and

wherein the second device includes a second management agent to receive management operations from the first management agent.

26. The system of claim 25, the first management agent to report back to the management console a status of management operations.

27. The system of claim 25, wherein the plurality of devices to be used by a user include at least one of a laptop computer, a desktop computer, a personal digital assistant, or a cell phone.

28. The system of claim 25, wherein the management authority is a management authority over platform managed resources.

29. The system of claim 28, wherein the platform managed resources include at least one of hardware, software, applications, or services.

30. The system of claim 25, the first user device further comprising a secure storage area to store a key, wherein the first management agent is to perform the management authority and operations in response to the stored key.

31. The system of claim 25, the plurality of devices further comprising a third device, wherein the second management agent is to perform management authority and operations on the third device in response to the received management operations.

32. The system of claim 25, the plurality of devices further comprising a third device, wherein the first management agent is to perform management authority and operations on the third device in response to the received management operations.

33. The system of claim 25, wherein the plurality of devices is a collection of devices to be used by an employee.

34. The system of claim 25, wherein the first management agent is to receive authority delegated from the management console to the first device to perform management operations on behalf of the management console on one or more other devices.

* * * * *