(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2017 (02.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/019075 A1

(51) International Patent Classification:
*G06F 21/86* (2013.01) *H05K 7/14* (2006.01)
*G06F 21/88* (2013.01)

(21) International Application Number:
PCT/US2015/042810

(22) International Filing Date:
30 July 2015 (30.07.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventor: **CAVANNA, Eric E.**; 8000 Foothills Blvd., Roseville, California 95747 (US).

(74) Agents: **KWOK, Jonathan T** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: LOCK CONTROL

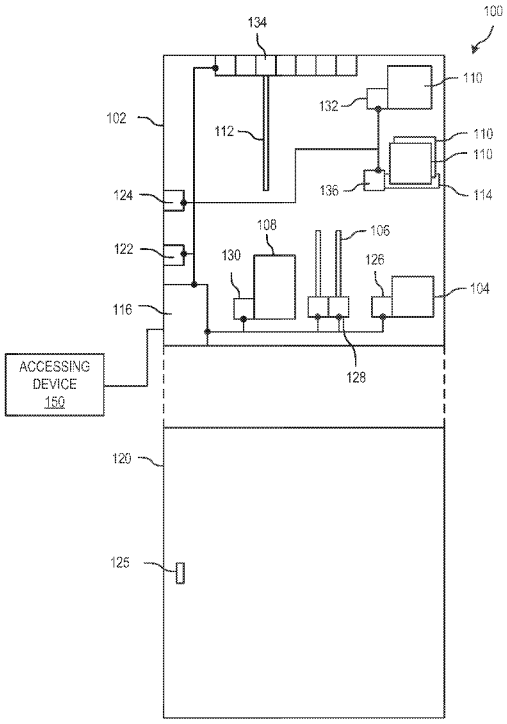


FIG. 1

(57) Abstract: Example implementations relate to a remote management controller of a computing system that receives a lock control command from an accessing device. The remote management controller may control an electronically controllable lock of the computing system according to the lock control command. For example, the electronically controllable lock may be a lid lock to secure a lid to a chassis of the computing system or a component lock to secure a component of the computing system.

WO 2017/019075 A1

**Declarations under Rule 4.17**:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

**Published**:

— *with international search report (Art. 21(3))*

# LOCK CONTROL

## BACKGROUND

[0001] A server may include various components, such as a circuit board, a processor, memory, a storage device, a graphics card, a network adapter, fans, and the like, disposed in a chassis. A lid may be placed on the chassis to form an enclosed server unit. A chassis may free standing or rack-mountable.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Various examples will be described below with reference to the following figures.

[0003] FIG. 1 is a diagram of an example computing system having electronically controllable locks, according to an implementation.

[0004] FIG. 2 is a diagram of an example computing system having electronically controllable locks, according to an implementation.

[0005] FIG. 3 is a flowchart of an example method for controlling electronically controllable locks, according to an implementation.

[0006] FIG. 4 is a flowchart of an example method for recording a state of electronically controllable locks, according to an implementation.

[0007] FIG. 5 is a flowchart of an example method for transmitting lock control options based on user privileges, according to an implementation.

[0008] FIG. 6 is a block diagram of an example remote management controller that includes a non-transitory, machine-readable medium encoded with instructions to control an electronically controllable lock, according to an implementation.

[0009] FIG. 7 is a block diagram of an example remote management controller that includes a non-transitory, machine-readable medium encoded with instructions to record a state of an electronically controllable lock, according to an implementation.

[0010] Throughout the drawings, identical reference numbers may designate similar, but not necessarily identical, elements.

## Detailed Description

[0011] A server may include a number of components disposed in a chassis. For example, the components of a server may include any number of: circuit boards (e.g., main system board, expansion board), processors, memory, storage devices, input/output (I/O) cards (e.g., a network adapter), cables, sockets, interconnects, heat management devices (e.g., fans), and the like. Some components may be wholly disposed within the chassis and thus be deemed internal components (e.g., a processor), and some components may be at least partially exposed to the exterior of the chassis (e.g., an I/O card or a removable storage media drive may be partially exposed so as to interface with other devices or a user). Some of the aforementioned components, such as a circuit board for example, may be mounted directly to the chassis. Other components may be mounted indirectly to the chassis, for example, by mounting to a socket on a circuit board that is mounted to the chassis or by mounting to a cartridge that is mounted to the chassis. Some components may be connected to each other, for example, by a socket, a cable, an interconnect component, or another connector.

[0012] The server chassis may be closed by a lid. The lid may be openable or removable so as to allow access to the components for maintenance, replacement, removal, and the like. However, high value components may be at risk for theft. Moreover, in some situations, removing or tampering with components at an improper time, such as during a server firmware upgrade, may be harmful to the operation of the server. To prevent unauthorized removal or tampering with the components, some chassis and lids may be equipped with a lock. The lid may be locked and unlocked using a key. Although such a key and lock system may prevent unauthorized access, a key may be misplaced or stolen. A key and lock system also may lack convenience, as sharing or delegation of chassis access is accomplished by physically sharing the key. Accordingly, a remote management controller

connected to locks of a computing system according to examples described herein may be useful for providing remote control, delegation, and monitoring of access to the components of a computing system.

[0013] Referring now to the figures, FIG. 1 is a diagram of an example computing system 100 having electronically controllable locks, according to an implementation. In some implementations, the computing system 100 may be a desktop computer, a workstation, a laptop computer, a server, a network switch, a storage array, or other like computing systems. The computing system 100 may include a chassis 102 to receive at least one component. In some implementations, the at least one component may be mounted or installed into the chassis 102, either directly or indirectly. In some implementations, the component may be deemed at least partially internal to the chassis 102 and, more generally, the computing system 100. In some implementations, the chassis 102 may be a free-standing chassis, a rack-mountable chassis, a blade, or other types of computing system chassis.

[0014] Examples of the at least one component may include a processor 104, memory 106 (e.g., a dual-inline memory module), and/or a storage device 108 (e.g., a hard disk drive, a solid state drive, a hard disk drive array, a tape drive, an optical drive, a removable media drive, or the like). The at least one component also may be a circuit board 110. Various implementations of the computing system 100 may include different types, combinations, or quantities of circuit boards 110, and examples of such circuit boards 110 may include a main system board (e.g., a motherboard), a power backplane board, an input/output (I/O) backplane board (e.g., which may include peripheral component interconnect (PCI) slots, PCI-X slots, PCI Express slots, or the like), a peripheral interface board (e.g., which may include keyboard, mouse, and Universal Serial Bus ports, or the like), a processor board, a memory board, or an expansion card 112 (also referred to as an I/O card, and may include, e.g., a PCI card, PCI-X card, PCI Express card, or the like). Other examples of components may include, for example, a power supply, a peripheral connector such as a Universal Serial Bus interface

with a peripheral device, a thermal management device such as a fan, and/or a component-to-component connector such as a cable, a circuit board interconnect 114, and/or the like.

[0015] The computing system 100 may also include a remote management controller 116. The remote management controller 116 may be implemented as a set of instructions encoded on a machine readable medium and executable by a processor (e.g., such as microprocessor, an application-specific integrated circuit, a field programmable gate array, and/or other hardware device suitable for retrieval and/or execution of instructions). Additionally or alternatively, the remote management controller 116 may be implemented as a hardware device comprising electronic circuitry. In some implementations, the remote management controller 116 may reside on a circuit board 110, which may be inside the chassis 102. In some implementations, the remote management controller 116 may be a lights out management controller or the like, and may include any kind of wired or wireless network interface to provide or form part of an out-of-band network path. For example, an accessing device 150, such as a desktop computer, a workstation, a laptop computer, a server, a smartphone, a tablet computer, or the like, that is external to the chassis 102 and separate from the computing system 100, may communicate with the remote management controller 116 via the out-of-band network path, such that a user of the accessing device 150 can remotely manage aspects of the computing system 100, such as firmware or hardware settings, remote rebooting, remote installation, system diagnostics, and logging. By virtue of communicating with the remote management controller 116 via the out-of-band network path, the user at the accessing device 150 may manage the computing system 100 during normal operation of the computing system 100, in the event of a failure of the computing system 100, or even when the computing system 100 has been powered off. In some implementations, the remote management controller 116 may maintain different user profiles for different users or groups of users. Each of the user profiles may have associated user privileges, and more particularly, the user privileges may be permission to perform some or all of

the remote management functions described above (e.g., managing firmware/hardware settings, remote rebooting, remote installation, system diagnostics, etc.). For example, some user profiles may be standard users and have a limited set of privileges, such as diagnostic privileges only. Other user profiles may be administrators and have a full set of privileges, including privileges to alter operation of the computing system 100 (e.g., managing firmware/hardware settings). As will be described further herein below, the remote management controller 116 also may provide its remote access and management functionality and user privilege sets to the management of electronically controllable locks of the computing system 100 and management of access to the components within the chassis 102.

[0016] The computing system 100 also may include a removable lid 120 to close the chassis 102. For example, the chassis 102 may have an opening by which components inside the chassis 102 may be accessed (e.g., for removal, servicing, configuring, etc.), and the lid 120 may be affixed to the chassis 102 to close the chassis 102 and enclose the components within the chassis 102. By virtue of closing the chassis 102 with the lid 120, at least some components inside the closed chassis 102 may be physically inaccessible until the lid 120 is removed or opened (with a possible example exception of portions of the components that are intentionally exposed to the exterior of the computing system 100, such as a port of an expansion card 112). The lid 120 is depicted in FIG. 1 as being removed from the chassis 102 (i.e., in an open position). In some implementations, a lid state sensor 122 may be disposed on the chassis 102 (or alternatively, on the lid 120). The lid state sensor 122 may detect when the lid 120 is open or closed with respect to the chassis 102, and indicate respectively a lid open state or a lid closed state to the remote management controller 116. For example, the lid state sensor 122 may be a magnetic or mechanical contact switch. In some implementations, the remote management controller 116 may store the lid open state or lid closed state information in an event log, together with time-stamps or other applicable log information, thus creating a historical record of the lid open or closed state. For example, the remote management controller

116 may store such an event log in non-volatile memory of the remote management controller 116 or in the storage device 108.

[0017] The computing system 100 also may include at least one electronically controllable lock, and more particularly, may include an electronic lid lock 124, at least one an electronic component lock (e.g., 126, 128, 130, 132, 134, or 136, to be described further herein below), or both an electronic lid lock 124 and at least one electronic component lock. The electronic locks may also be referred to as electronically controllable locks. The electronic lid lock and the electronic component lock may be collectively referred to herein as "the locks." In some implementations, the computing system 100 may include an electronic lid lock 124 to secure the lid 120 to the chassis 102. For example, the electronic lid lock 124 may be a solenoid bolt lock, a motorized rotary lock, or the like, and may be disposed or mounted in or on the chassis 102. In response to a lock or unlock signal (e.g., a digital signal, an analog signal, a voltage signal, etc.), the electronic lid lock 124 may engage a complementary catch 125 on the lid 120 to secure the lid 120 to the chassis 102 or may disengage the catch 125 to allow the lid 120 to be removed, respectively. Alternatively, in some implementations, the electronic lid lock may be disposed on the lid 120 and the catch may be disposed on the chassis 102. In yet other implementations, both the electronic lid lock and the catch may be disposed on the lid 120 (or alternatively, in or on the chassis 102), and engaging the electronic lid lock to the catch may prevent the lid 120 from being removed, while disengaging the electronic lid lock from the catch may allow the lid 120 to be removed. Other electronic lid lock mechanisms may be suitable to secure the lid 120 to the chassis 102.

[0018] In some implementations, the computing system 100 includes an electronic component lock disposed in or on the chassis 102 to secure a component, and more particularly, to secure the component to the chassis 102. For example, in the illustrated example of FIG. 1, an electronic component lock 126 may secure the processor 104, an electronic component lock 128 may secure the memory 106, an electronic component lock 130 may

secure the storage device 108, an electronic component lock 132 may secure a circuit board 110, an electronic component lock 134 may secure an I/O or expansion card 112, and an electronic component lock 136 may secure the circuit board interconnect 114. It should be understood that different implementations of the computing system 100 may include more or fewer of the electronic component locks illustrated in FIG. 1. An electronic component lock may be a solenoid bolt lock, a motorized rotary lock, or the like, that engages, clamps, or physically integrates with the corresponding component in response to a lock signal, and disengages, unclamps, or disconnects from the corresponding component in response to an unlock signal. The specific type of lock may depend on the size, shape, position, or other characteristic of the corresponding component that it secures. In some implementations, an electronic component lock may secure multiple components.

[0019] Some of the aforementioned electronic component locks may secure a corresponding component to the chassis 102 directly, for example, where the lock itself is mounted securely to the chassis 102 and the lock engages the component so as to secure the component to the chassis 102. Others of the aforementioned electronic component locks may secure the corresponding component to the chassis 102 indirectly, for example, by securing the component to a socket, a cartridge, or the like, which in turn is either mounted securely to the chassis 102 or secured by another lock to the chassis 102. In some implementations, the electronic component lock 136 circuit board interconnect 114 may secure two or more interconnected circuit boards 110 to each other. Other components not shown on FIG. 1, such as a power supply, a peripheral connector, a thermal management device, or a cable, may be understood to also be securable to the chassis 102 by an electronic component lock in a manner described above.

[0020] In some implementations, the remote management controller 116 may be connected to the locks. In some implementations, the remote management controller 116 may control the locking or unlocking of each of the electronic lid lock 124 and/or the electronic component lock 126, 128, 130,

132, 134, 136 independently, by transmitting a lock or unlock signal (as described above) to individual ones of the locks. The lock or unlock signal may be a digital signal, an analog signal, a voltage signal, etc., depending on the type of lock. In some implementations, each of the locks may indicate their respective locked or unlocked state to the remote management controller 116. More particularly, the remote management controller 116 may poll (or query or read) the locked or unlocked state of the locks, or the locks may report their respective locked or unlocked states to the remote management controller 116. In some implementations, the remote management controller 116 may store the locked states or unlocked states of the locks in the aforementioned event log, thus creating a historical record of the locked or unlocked states.

[0021] In some implementations, the remote management controller 116 may receive a lock control command from the accessing device 150 external to the chassis 102, and may control the electronic lid lock 124 or the electronic component lock 126, 128, 130, 132, 134, 136 according to the lock control command. For example, the lock control command may be a command (e.g., an Application Programming Interface, or API, function call; an electronic instruction; a control signal; etc.) to lock or unlock a particular lock of the locks. In some implementations, the lock control command may be a real-time command that the remote management controller 116 carries out upon receipt (or as soon as possible after receipt) from the accessing device 150. In some implementations, the lock control command may include a time, date, or a delay to schedule when the remote management controller 116 will lock or unlock a particular lock of the locks. In some implementations, the lock control command may include an event trigger that the remote management controller 116 waits for before locking or unlocking a particular lock of the locks. For example, the lock control command may instruct the remote management controller 116 to lock the electronic lid lock 124 upon detection of a lid closed state (by the lid state sensor 122) or upon a change from a lid open state to a lid closed state. In some implementations, the lock control command may confirm whether the lock control command has been

successfully carried out (e.g., by polling the state of the lock identified in the lock control command and/or by polling the lid state sensor 122) and send a success or failure response to the accessing device 150 accordingly.

[0022] The remote management controller 116 also may transmit the event log (containing historical information about the lid open state, lid closed state, locked states of the locks, and/or unlocked states of the locks) to the accessing device 150, via the out-of-band network path or another wired or wireless network path. For example, the event log may be transmitted in response to an event log request from the accessing device 150. In some implementations, the event log may be transmitted as a report or as raw data. In some implementations, the remote management controller 116 may send a notification (or an alert) related to a lid open state, a lid closed state, a locked state, or an unlocked state. For example, the remote management controller 116 may be configured to send such a notification at the moment the lid 120 is opened, if the lid 120 is left opened for a predefined period of time (e.g., 1 hour, 24 hours, or another period), at the moment a lock is opened, or if a lock is left in its unlocked state for a predefined period of time (e.g., 1 hour, 24 hours, or another period). A notification may also be sent when the lid 120 is closed or a lock is set to their locked state. The notification may be, for example, an email, an instant messaging service notification, a short message service notification, a multimedia message service notification, a voice or audio message, a programmatic message (e.g., an HTTP request), or the like. In some implementations, the notification may be addressed to a designated recipient (or recipients), such as an administrator or a person who oversees or audits access to the computing system 100. To send the notification, the remote management system 116 may include on-board email or message sending capabilities, or may access external email or message sending services via application program interfaces of those external services.

[0023] In some implementations, the remote management controller 116 may administer (or apply or enforce) user privileges related to the electronic lid lock 124 or the electronic component lock 126, 128, 130, 132, 134, 136.

Such lock-related user privileges may be associated with the aforementioned user profiles of the remote management controller 116. For example, an administrator user profile may have a full set of system administration privileges as described above (e.g., managing firmware/hardware settings, etc.) and may also have full privileges to manage the locks, while a standard user profile may have limited or no privileges to manage operation of the computing system 100 or the locks. For example, administrator user profiles may have user privileges to lock or unlock the locks at any time, and accordingly, the remote management controller 116 may control the locks according to a lock control command from such administrator users at any time. Some standard user profiles may have user privileges to lock or unlock the locks according to a schedule, such as during weekday working hours (e.g., 8:00 AM to 5:00 PM, Monday through Friday), and accordingly, the remote management controller 116 may control the locks according to a lock control command from such standard users only during the scheduled times and may ignore lock control commands during other times. In another example, some user profiles may have privileges to lock the locks but not unlock the locks. In another example, some user profiles may have privileges to request or access the event log. In another example, some user profiles, such as administrators, may have user privileges to create user profiles or to modify the user privileges of existing user profiles, including the schedule according to which those user profiles may lock or unlock the locks. Some user profiles may have user privileges to modify the configuration of the remote management controller 116, such as how the event log or notifications are sent (e.g., via email, message, to the accessing device 150, etc.), the contact information of the designated recipient (e.g., email address, phone number, short message service number or address, etc.), when the event log or notifications are sent, and other lock-related rules. In some implementations, the remote management controller 116 may send a notification to a designated recipient (e.g., in a manner similar to that described above) in response to changes in user privileges.

[0024] In some implementations, the remote management controller 116 may respond or react to predetermined events of the computing system 100. For example, the remote management controller 116 may temporarily alter (e.g., revoke or suspend) user privileges to lock or unlock the electronic lid lock 124 or the electronic component lock 126, 128, 130, 132, 134, 136 during predetermined events (or states) of the computing system 100. In some implementations, such alteration of privileges may also apply to administrator level user profiles. In some implementations, the remote management controller 116 may lock the electronic lid lock 124 or the electronic component lock 126, 128, 130, 132, 134, 136 during or in response to the predetermined events, automatically or independent of a lock control command. The remote management controller 116 also may unlock the locks after the predetermined event has completed. Examples of predetermined events that may trigger temporary alteration of user privileges or locking of a lock include events where removal of a component of the computing system 100 may damage or otherwise interfere with operation of the computing system 100 (even if the component is hot-swappable, for example), such as during a firmware upgrade process, during a safety-critical or life-critical operation, in a high-availability system, or the like. At least some of the foregoing predetermined events also may be used as the above-described event trigger included in a lock control command received from the accessing device 150.

[0025] In some implementations, the predetermined events may be preprogrammed into the remote management controller 116, and the remote management controller 116 may monitor the computing system 100 for the events. In some implementations, the computing system 100 (or more particularly, an operating system, an application, or the like, executing on the computing system 100) may cause the predetermined events, and the source of the predetermined event may instruct the remote management controller 116 to alter privileges or lock or unlock a lock. To illustrate, a firmware update application executing on the computing system 100 may be designed to instruct the remote management controller 116 (e.g., via an API function call, which may differ from the lock control command API function call) to lock

some or all of the locks prior to updating firmware, and then may instruct the remote management controller 116 to unlock those locks after the firmware update is complete.

[0026] In some implementations, the remote management controller 116 may transmit options related to the above described user privileges to the accessing device 150. The options transmitted may depend on the privileges of the user profile logged on to the remote management controller 116 through the accessing device 150. The accessing device 150 may present the options to the user operating the accessing device 150, on a display for example, and at least some of the options may be selectable. In some implementations, In some implementations, the remote management controller 116 may include an embedded web server that transmits the options, the event log, a present state of the lid or the locks, and other information to the accessing device 150 as a web page, JavaScript Object Notation data, Extensible Markup Language data, or the like. In some implementations, the remote management controller 116 may receive the lock control command from the accessing device 150 based on the transmitted options via the web page.

[0027] FIG. 2 is a diagram of an example computing system 200 having electronically controllable locks, according to an implementation. The computing system 200 includes a chassis 202 to receive a component 204 (e.g., a processor, memory, a storage device, a circuit board, etc.) and a removable lid 206 to close the chassis 204. The computing system 200 also includes an electronic lid lock 208 to secure the lid 206 to the chassis 202 and an electronic component lock 210 disposed in or on the chassis 202 to secure the component 204. The computing system 200 also includes a remote management controller 212 to receive a lock control command from an accessing device 220 external to the chassis 202 and to control the electronic lid lock 208 or the electronic component lock 210 according to the lock control command. In some implementations, the electronic lid lock 208 may be

disposed in or on the chassis 202. In some implementations, the remote management controller 212 may be included inside the chassis 202.

[0028] FIG. 3 is a flowchart of an example method 300 for controlling electronically controllable locks, according to an implementation. Method 300 may be described below as being executed or performed by a remote management controller 116 of a computing system 100 described above with respect to FIG. 1. Various other remote management controllers may be used as well, such as, for example, the remote management controller 212 of FIG. 2. Method 300 may be implemented in the form of executable instructions stored on a machine-readable storage medium and executed by at least one processor of the remote management controller 116, and/or in the form of electronic circuitry. In some implementations of the present disclosure, one or more blocks of method 300 may be executed substantially concurrently or in a different order than shown in FIG. 3. In some implementations of the present disclosure, method 300 may include more or fewer blocks than are shown in FIG. 3. In some implementations, one or more of the blocks of method 300 may, at certain times, be ongoing and/or may repeat.

[0029] The method 300 may begin at block 302, and continue to block 304, where a remote management controller 116 of a computing system (e.g., 100) may receive a lock control command via an out-of-band network transmission. For example, the lock control command may be transmitted by an accessing device (e.g., 150) and may be a command to lock or unlock an electronically controllable lock of the computing system 100. At block 306, the remote management controller 116 may control electronically controllable locks of a chassis (e.g., 102) of the computing system 100 according to the lock control command received at block 304. In some implementations, the electronically controllable locks may include a lid lock (e.g., 124) to secure a lid (e.g., 120) to the chassis and a component lock (e.g., 126, 128, 130, 132, 134, 136) to secure a component (e.g., 104, 106, 108, 110, 112, 114) of the computing system to, for example, the chassis. At block 308, the method 300 may end.

[0030] FIG. 4 is a flowchart of an example method for recording a state of electronically controllable locks, according to an implementation. Method 400 may be described below as being executed or performed by a remote management controller 116 of a computing system 100 described above with respect to FIG. 1. Various other remote management controllers may be used as well, such as, for example, the remote management controller 212 of FIG. 2. Method 400 may be implemented in the form of executable instructions stored on a machine-readable storage medium and executed by at least one processor of the remote management controller 116, and/or in the form of electronic circuitry. In some implementations of the present disclosure, one or more blocks of method 400 may be executed substantially concurrently or in a different order than shown in FIG. 4. In some implementations of the present disclosure, method 400 may include more or fewer blocks than are shown in FIG. 4. In some implementations, one or more of the blocks of method 400 may, at certain times, be ongoing and/or may repeat.

[0031] The method 400 may begin at block 402, and continue to block 404, where the remote management controller 116 of a computing system (e.g., 100) may record an open state of a lid (e.g., 120), a closed state of the lid, locked states of electronically controllable locks (e.g., 124, 126, 128, 130, 132, 134, 136), or unlocked states of the electronically controllable locks, in an event log. For example, the event log may be stored in a non-volatile memory of the remote management controller 116 or in a storage device available to the computing system (e.g., a hard drive, a solid state drive, a removable media drive, a networked storage, etc.). At block 406, the remote management controller 116 may generate a report based on the event log. For example, the report may be raw data from the event log (or a portion thereof) or may be a summary of the event log (or a portion thereof), and may be a data file, an email, or other type of electronic document (e.g., a JavaScript Object Notation file or Extensible Markup Language file). At block 408, the remote management controller 116 may transmit the report generated at block 406 to an accessing device (e.g., 150) or a designated

recipient. For example, the remote management controller 116 may transmit the report via an out-of-band network path or another wired or wireless network path. In some implementations, the report may be transmitted in response to a report request from the accessing device or the designated recipient. In some implementations, the report may be transmitted to the accessing device or the designated recipient at scheduled times. The designated recipient may be, for example, an administrator of the computing system 100 or a person who audits access to the computing system 100. At block 410, the method 400 may end.

[0032] FIG. 5 is a flowchart of an example method for transmitting lock control options based on user privileges, according to an implementation. Method 500 may be described below as being executed or performed by a remote management controller 116 of a computing system 100 described above with respect to FIG. 1. Various other remote management controllers may be used as well, such as, for example, the remote management controller 212 of FIG. 2. Method 500 may be implemented in the form of executable instructions stored on a machine-readable storage medium and executed by at least one processor of the remote management controller 116, and/or in the form of electronic circuitry. In some implementations of the present disclosure, one or more blocks of method 500 may be executed substantially concurrently or in a different order than shown in FIG. 5. In some implementations of the present disclosure, method 500 may include more or fewer blocks than are shown in FIG. 5. In some implementations, one or more of the blocks of method 500 may, at certain times, be ongoing and/or may repeat.

[0033] The method 500 may begin at block 502, and continue to block 504, where the remote management controller 116 of a computing system (e.g., 100) may maintain (or store or administer) user profiles, each of the user profiles having associated user privileges. For example, as described above with respect to FIG. 1, some user profiles may have more of less user privileges than other user profiles. In some implementations, the user

privileges may include privileges to lock or unlock electronically controllable locks of the computing system (and more particularly, at or during all times or according to a schedule), privileges to modify the user privileges of user profiles, or other privileges. At block 506, the remote management controller 116 may receive, from an accessing device (e.g., 150) external to the computing system, authentication data for a user profile (e.g., a user name and password, or the like). For example, a user of the accessing device may enter authentication data at the accessing device, and the accessing device may transmit the authentication data via an out-of-band network path or another wired or wireless network path to the remote management controller 116. At block 508, the remote management controller 116 may transmit to the accessing device, lock control options based on the user privileges associated with the user profile. In some implementations, the remote management controller 116 may transmit the lock control options as a web page for display on the accessing device, and the lock control options may include options to lock at least one of the electronically controllable locks, to unlock at least one of the electronically controllable locks, to modify lock-related user privileges of user profiles, to modify configuration details of the remote management controller 116, or to request a report based on an event log. The remote management controller 116 may transmit different lock control options depending on the logged on user profile. For example, if the authentication data correspond to an administrator user profile, the remote management controller 116 may transmit a full set of lock control options. On the other hand, if the authentication data correspond to a standard or lower level user profile, the remote management controller 116 may transmit a more limited set of lock control options (e.g., a lock option, but no unlock option; lock and/or unlock options only during scheduled times). At block 510, the method 500 may end.

[0034] FIG. 6 is a block diagram illustrating a remote management controller 600 that includes a machine-readable medium encoded with instructions to control an electronically controllable lock, according to an implementation. In some implementations, the remote management controller

600 may serve as or form part of the remote management controller 116 of FIG. 1 or the remote management controller 212 of FIG. 2. In some implementations, the remote management controller 600 may include at least one processor 602 coupled to a machine-readable medium 604. The processor 602 may include a single-core processor, a multi-core processor, an application-specific integrated circuit, a field programmable gate array, and/or other hardware device suitable for retrieval and/or execution of instructions from the machine-readable medium 604 (e.g., instructions 606, 608, 610, 612) to perform functions related to various examples. Additionally or alternatively, the processor 602 may include electronic circuitry for performing the functionality described herein, including, but not limited to, the functionality of instructions 606, 608, 610, and/or 612. With respect to the executable instructions represented as boxes in FIG. 6, it should be understood that part or all of the executable instructions and/or electronic circuits included within one box may, in alternate implementations, be included in a different box shown in the figures or in a different box not shown. In some implementations, the remote management controller 600 may be installed or disposed in a computing system (e.g., computing system 100 or 200) and may be connected to at least one electronically controllable lock of the computing system. For example, the electronically controllable lock may include a lid lock to secure a lid to a chassis of the computing system, or a component lock to secure a component of the computing system (e.g., a processor, memory, a storage device, a circuit board, etc.) to the chassis. In some implementations, the remote management controller 600 may communicate with an accessing device (e.g., a device that is separate from the computing system) via an out-of-band network path.

[0035] The machine-readable medium 604 may be any medium suitable for storing executable instructions, such as random access memory (RAM), electrically erasable programmable read-only memory (EEPROM), flash memory, hard disk drives, optical discs, and the like. In some example implementations, the machine-readable medium 604 may be a tangible, non-transitory medium, where the term “non-transitory” does not encompass

transitory propagating signals. As described further herein below, the machine-readable medium 604 may be encoded with a set of executable instructions 606, 608, 610, 612.

[0036] Instructions 606, when executed by the processor 602, may receive, from an accessing device, authentication data for a user profile (e.g., a user name and password). In some implementations, the remote management controller 600 may store user profiles and user privileges associated with those user profiles.

[0037] Instructions 608, when executed by the processor 602, may transmit, to the accessing device, lock control options based on user privileges associated with the user profile (e.g., the user profile associated with the authentication data received by instructions 606). For example, the user privileges may include a privilege to lock an electronically controllable lock of the computing system in which the remote management controller 600 is installed or a privilege to unlock the electronically controllable lock, and the transmitted lock control options may be a lock option or an unlock option, respectively. In some instances, a user privilege may include privileges to lock or unlock the electronically controllable lock according to a schedule, and instructions 608 may transmit lock or unlock options if the schedule indicates the user profile is allowed to perform those operations at the present time (e.g., at the time the authentication data is received). In some implementations, the user privileges may include privileges to lock or unlock particular ones of a plurality of electronically controllable locks (e.g., a lid lock 124, a processor lock 126, a memory lock 128, etc.) but not others of the electronically controllable locks, and instructions 608 may transmit lock or unlock options for each of the particular electronically controllable locks. In some implementations, the user privileges may include a privilege to alter user privileges of user profiles or configuration details of the remote management controller 116, and instructions 608 may transmit the configurable options for those user privileges or the remote management controller 116. In some implementations, the accessing device may present

the privilege-based lock control options to a user (e.g., as buttons or text on a display), and the user may make a selection from among the lock control options at the accessing device.

[0038] Instructions 610, when executed by the processor 602, may receive a lock control command (e.g., an API function call, an electronic instruction, a control signal, etc.). For example, the lock control command may be received from the accessing device and may relate to the selection made by the user from among the lock control options. As another example, the accessing device may run a script or an application to interface with the remote management controller 116 (e.g., without user input), and the script or application may be designed or programmed to recognize lock control options transmitted by instructions 608 and generate a lock control command in response to those lock control options. Instructions 612, when executed by the processor 602, may control an electronically controllable lock of the computing system according to the received lock control command.

[0039] FIG. 7 is a block diagram illustrating a remote management controller 700 that includes a machine-readable medium encoded with instructions to record a state of an electronically controllable lock, according to an implementation. The remote management controller 700 includes a processor 702 and a machine-readable medium 704, which may be analogous in many respects to the processor 602 and the machine-readable medium 604, respectively. The machine-readable medium 704 may be encoded with a set of executable instructions 706, 708, 710, 712. Additionally or alternatively, the processor 702 may include electronic circuitry for performing the functionality described herein, including, but not limited to, the functionality of instructions 706, 708, 710, 712. Similar to the remote management controller 600, the remote management controller 700 may be connected to at least one electronically controllable lock of the computing system, such as a lid lock to secure a lid to a chassis of a computing system or a component lock to secure a component of the computing system to the chassis.

[0040] Instructions 706, when executed by the processor 702, may record, in an event log, an open state of the lid, a closed state of the lid, a locked state of the electronically controllable lock, or an unlocked state of the electronically controllable lock. Instructions 708, when executed by the processor 702, may generate a report based on the event log. Instructions 710, when executed by the processor 702, may transmit the report to an accessing device or a designated recipient. For example, the report may be transmitted in response to a request or on a scheduled basis. Instructions 712, when executed by the processor 702, may send a notification related to the open state of the lid, the closed state of the lid, the locked state of the electronically controllable lock, the unlocked state of the electronically controllable lock, or changes in user privileges. For example, the notification may be sent in response to the lid being opened or if the lid is in an open state for a predetermined amount of time.

[0041] In view of the foregoing description, it can be appreciated that a lid lock or component locks of a computing system, and thus access to components of the computing system, may be controlled remotely and programmatically. Moreover, control of the locks may be delegated by modifying or creating user profiles to have the appropriate user privileges for controlling the locks, and more particularly, such delegated user privileges may be altered or restricted according to a schedule. Furthermore, by virtue of the remote management controller recording lid states (open/closed) or lock states (lock/unlock) in an event log, access to the components of the computing system 100 may be audited and monitored.

[0042] In the foregoing description, numerous details are set forth to provide an understanding of the subject matter disclosed herein. However, implementation may be practiced without some or all of these details. Other implementations may include modifications and variations from the details discussed above. It is intended that the following claims cover such modifications and variations.

We claim:

1. A system comprising:

a chassis to receive a component;

a removable lid to close the chassis;

an electronic lid lock to secure the lid to the chassis;

an electronic component lock disposed in or on the chassis to secure the component; and

a remote management controller to:

receive a lock control command from an accessing device external to the chassis, and

control the electronic lid lock or the electronic component lock according to the lock control command.

2. The system of claim 1, further comprising a lid state sensor to indicate a lid open state or a lid closed state to the remote management controller,

wherein the electronic lid lock and the electronic component lock are to indicate their respective locked or unlocked states to the remote management controller.

3. The system of claim 1, wherein the component includes a processor, memory, a storage device, a peripheral connector, a cable, a circuit board, a circuit board interconnect, or an expansion card.

4. The system of claim 2, wherein

the remote management controller is to store in an event log information including lid open state, lid closed state, locked states, or unlocked states, and is to transmit the event log to the accessing device, and

the remote management controller is to send a notification related to a lid open state, a lid closed state, a locked state, or an unlocked state.

5. The system of claim 4, wherein the notification is an email, an instant messaging service notification, a short message service notification, or a multimedia messaging service notification addressed to a designated recipient.

6. The system of claim 1, wherein the remote management controller is to administer user privileges related to the electronic lid lock or the electronic component lock, and is to send a notification to a designated recipient in response to changes in user privileges.

7. The system of claim 1, wherein the remote management controller is to temporarily alter user privileges to lock or unlock the electronic lid lock or the electronic component lock during predetermined events of the system,

or is to lock the electronic lid lock or the electronic component lock in response to predetermined events of the system.

8. A method comprising:

receiving, by a remote management controller of a computing system, a lock control command via an out-of-band network transmission; and

controlling, by the remote management controller, electronically controllable locks of a chassis of the computing system according to the received lock control command, the electronically controllable locks including a lid lock to secure a lid to the chassis and a component lock to secure a component of the computing system.

9. The method of claim 8, further comprising:

recording, by the remote management controller, an open state of the lid, a closed state of the lid, locked states of the electronically controllable locks, or unlocked states of the electronically controllable locks, in an event log;

generating, by the remote management controller, a report based on the event log; and

transmitting, by the remote management controller, the report to an accessing device or a designated recipient.

10. The method of claim 8, further comprising:

maintaining user profiles by the remote management controller, each of the user profiles having associated user privileges;

receiving, by the remote management controller from an accessing device external to the computing system, authentication data for a user profile; and

transmitting, by the remote management controller to the accessing device, lock control options based on the user privileges associated with the user profile.

11. The method of claim 10, wherein the lock control options include options to lock at least one of the electronically controllable locks, to unlock at least one of the electronically controllable locks, to modify lock-related user privileges of user profiles, or to request a report based on an event log.

12. The method of claim 10, wherein the user privileges include privileges to lock or unlock the electronically controllable locks according to a schedule, or privileges to modify the user privileges of user profiles.

13. A non-transitory machine readable medium, storing instructions executable by a processor of a remote management controller for a computing system, the non-transitory machine readable medium comprising:

instructions to receive, from an accessing device, authentication data for a user profile;

instructions to transmit, to the accessing device, lock control options based on user privileges associated with the user profile;

instructions to receive a lock control command; and

instructions to control an electronically controllable lock of the computing system according to the received lock control command,

wherein the user privileges include a privilege to lock or unlock the electronically controllable lock according to a schedule.

14. The non-transitory machine readable medium of claim 13, the electronically controllable lock includes a lid lock to secure a lid to a chassis of the computing system, or a component lock to secure a component of the computing system to the chassis.

15. The non-transitory machine readable medium of claim 14, further comprising:

instructions to record, in an event log, an open state of the lid, a closed state of the lid, a locked state of the electronically controllable lock, or an unlocked state of the electronically controllable lock;

instructions to generate a report based on the event log;

instructions to transmit the report to the accessing device or a designated recipient; and

instructions to send a notification related to the open state of the lid, the closed state of the lid, the locked state of the electronically controllable lock, the unlocked state of the electronically controllable lock, or changes in user privileges.

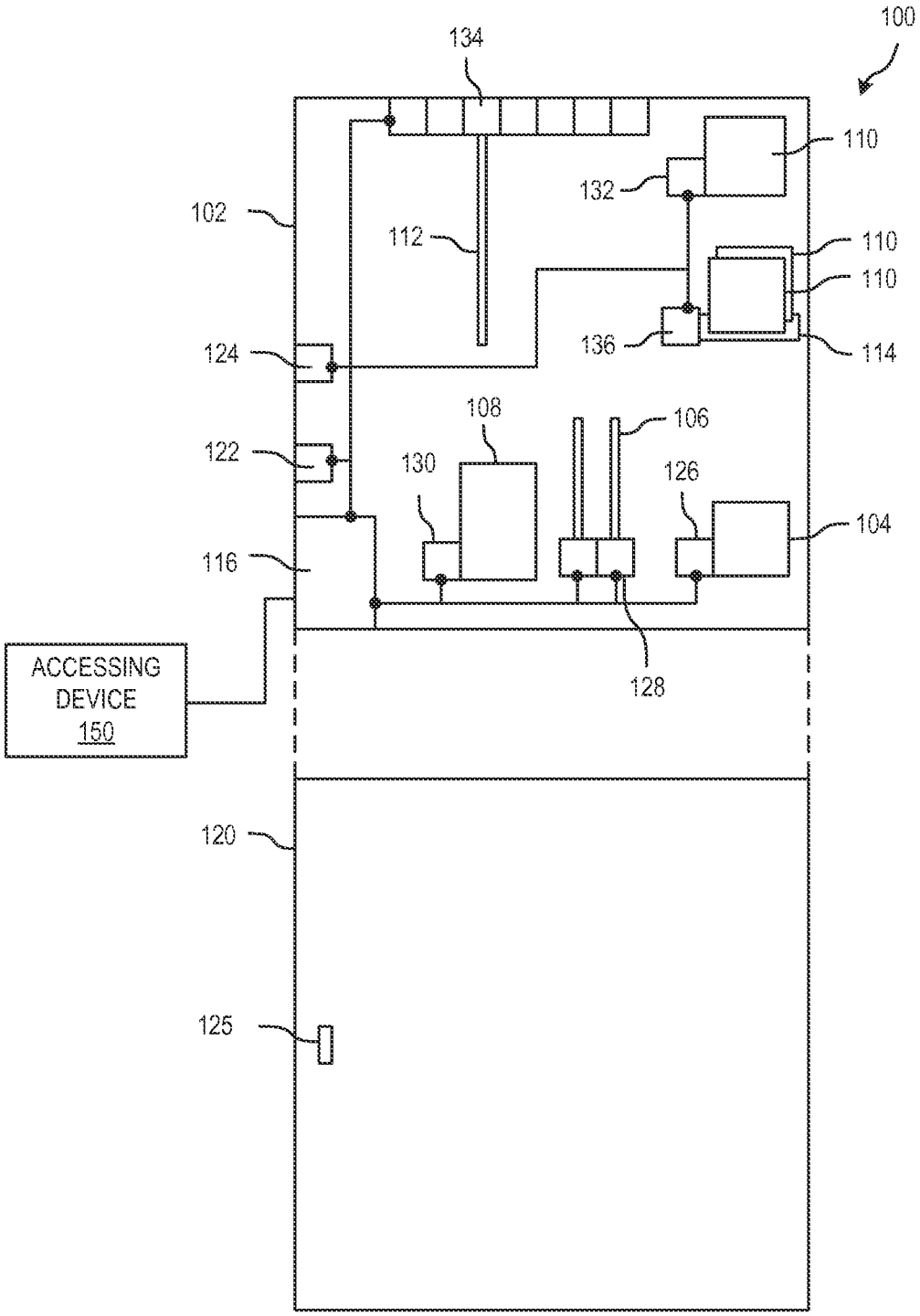
100
134
110
132
102
112
110
110
136
114
124
108
106
122
130
126
104
116
ACCESSING DEVICE 150
128
120
125

FIG. 1

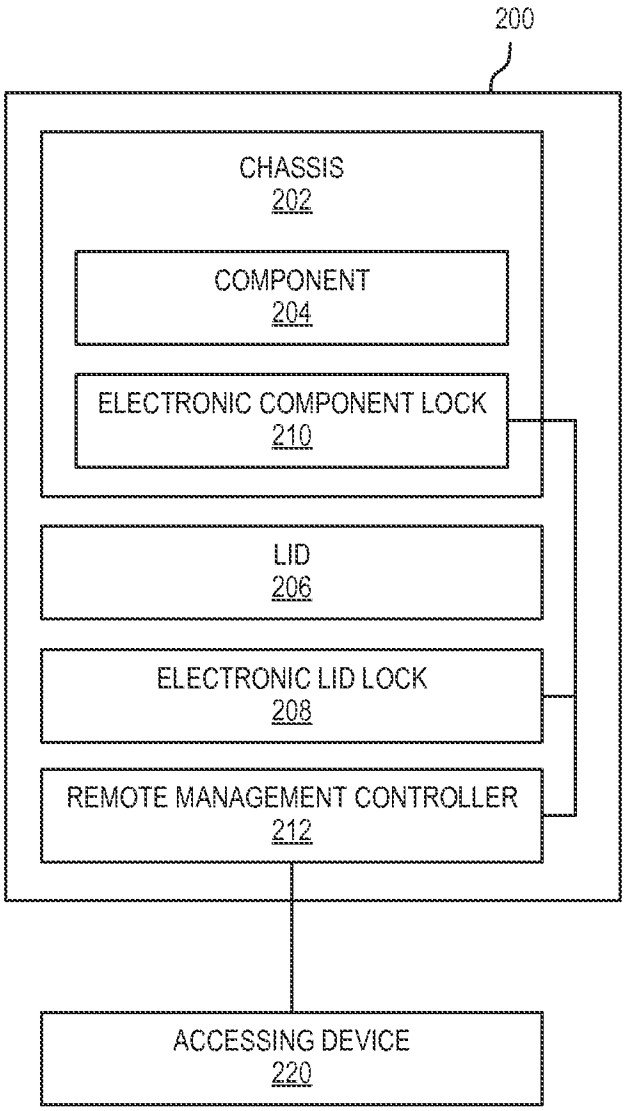
200
CHASSIS
202
COMPONENT
204
ELECTRONIC COMPONENT LOCK
210
LID
206
ELECTRONIC LID LOCK
208
REMOTE MANAGEMENT CONTROLLER
212
ACCESSING DEVICE
220

FIG. 2

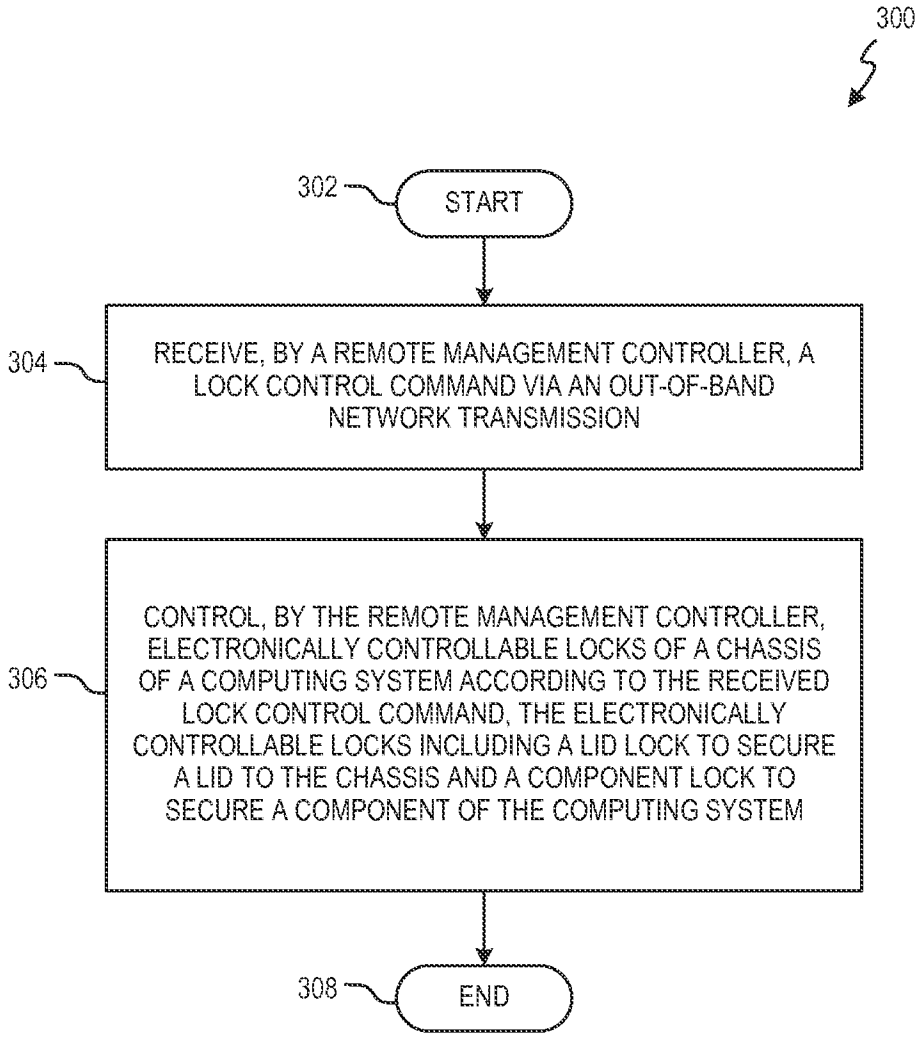
300
302
START
304
RECEIVE, BY A REMOTE MANAGEMENT CONTROLLER, A LOCK CONTROL COMMAND VIA AN OUT-OF-BAND NETWORK TRANSMISSION
306
CONTROL, BY THE REMOTE MANAGEMENT CONTROLLER, ELECTRONICALLY CONTROLLABLE LOCKS OF A CHASSIS OF A COMPUTING SYSTEM ACCORDING TO THE RECEIVED LOCK CONTROL COMMAND, THE ELECTRONICALLY CONTROLLABLE LOCKS INCLUDING A LID LOCK TO SECURE A LID TO THE CHASSIS AND A COMPONENT LOCK TO SECURE A COMPONENT OF THE COMPUTING SYSTEM
308
END

*FIG. 3*

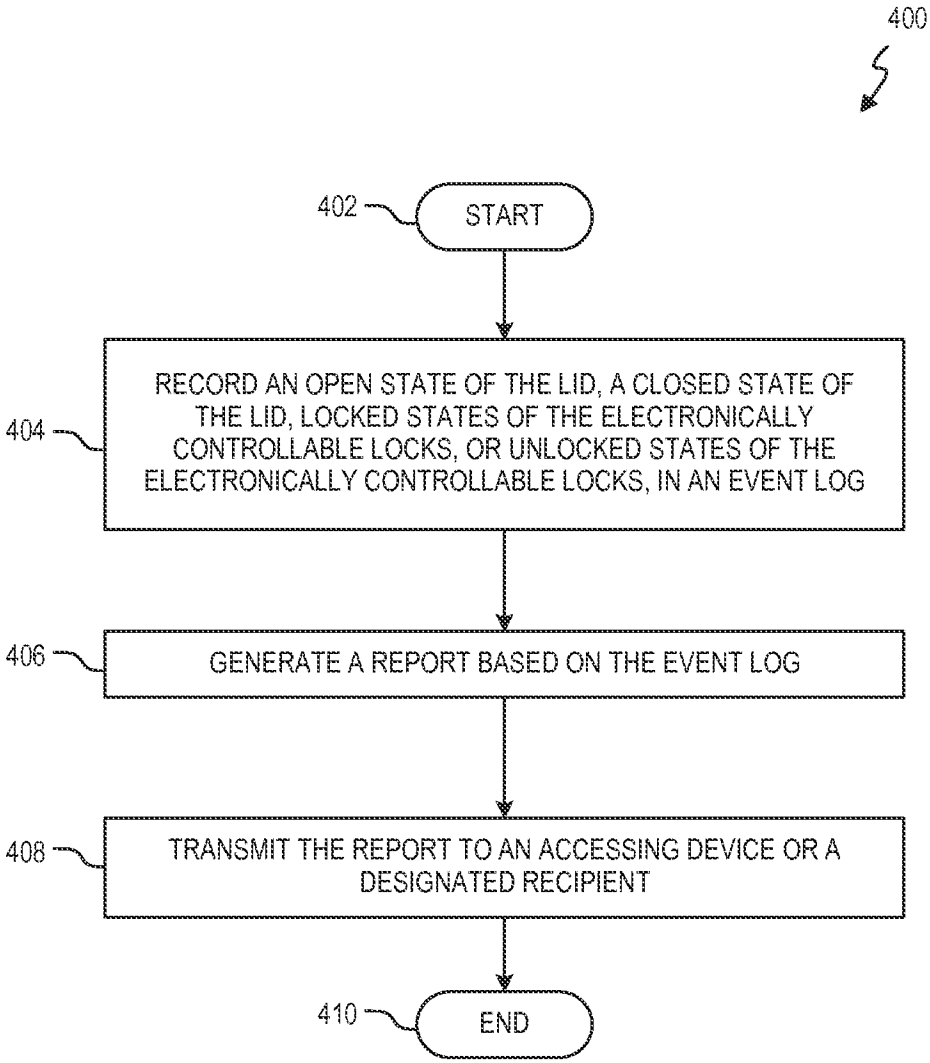
400
402
START
RECORD AN OPEN STATE OF THE LID, A CLOSED STATE OF THE LID, LOCKED STATES OF THE ELECTRONICALLY CONTROLLABLE LOCKS, OR UNLOCKED STATES OF THE ELECTRONICALLY CONTROLLABLE LOCKS, IN AN EVENT LOG
404
GENERATE A REPORT BASED ON THE EVENT LOG
406
TRANSMIT THE REPORT TO AN ACCESSING DEVICE OR A DESIGNATED RECIPIENT
408
410
END

FIG. 4

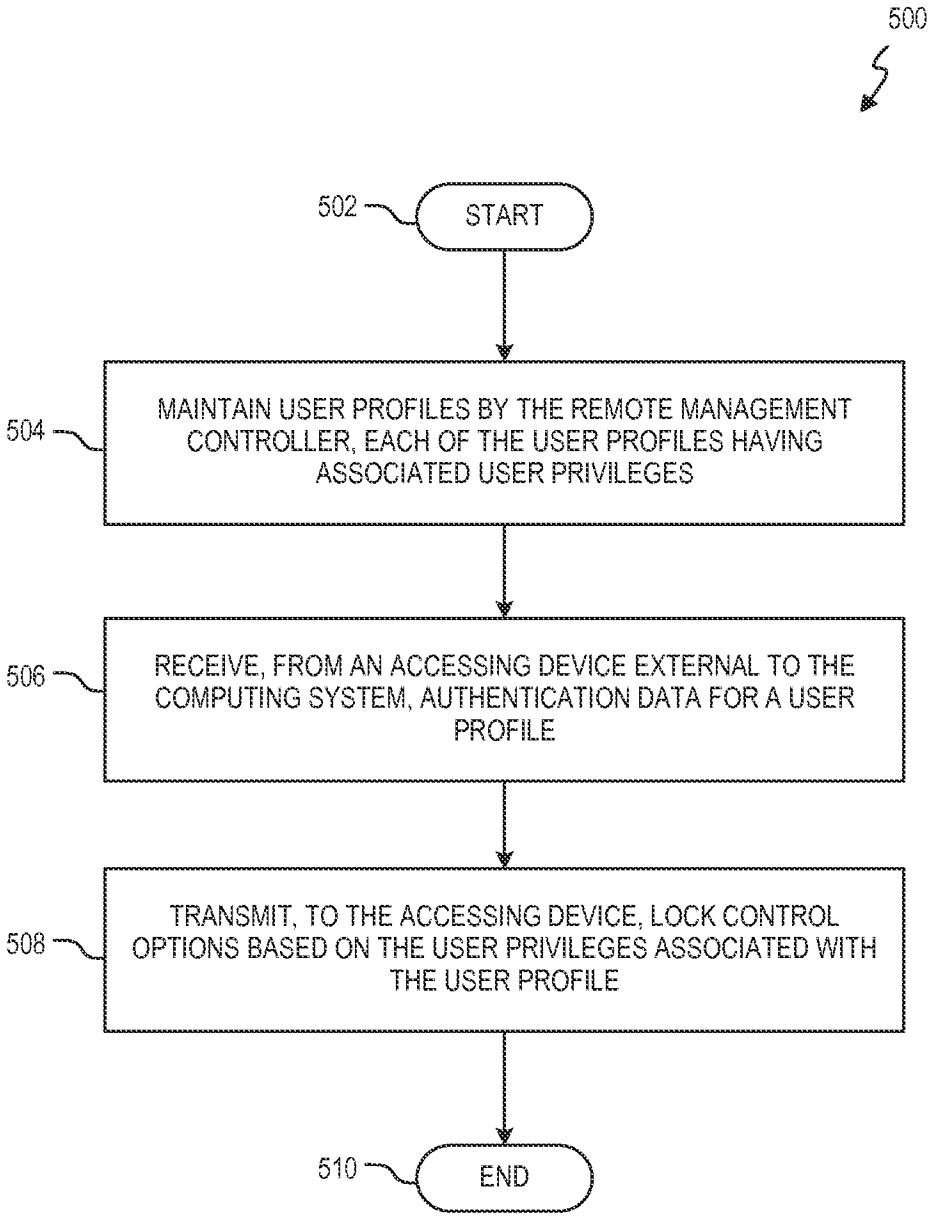
500
502
START
504
MAINTAIN USER PROFILES BY THE REMOTE MANAGEMENT CONTROLLER, EACH OF THE USER PROFILES HAVING ASSOCIATED USER PRIVILEGES
506
RECEIVE, FROM AN ACCESSING DEVICE EXTERNAL TO THE COMPUTING SYSTEM, AUTHENTICATION DATA FOR A USER PROFILE
508
TRANSMIT, TO THE ACCESSING DEVICE, LOCK CONTROL OPTIONS BASED ON THE USER PRIVILEGES ASSOCIATED WITH THE USER PROFILE
510
END

FIG. 5

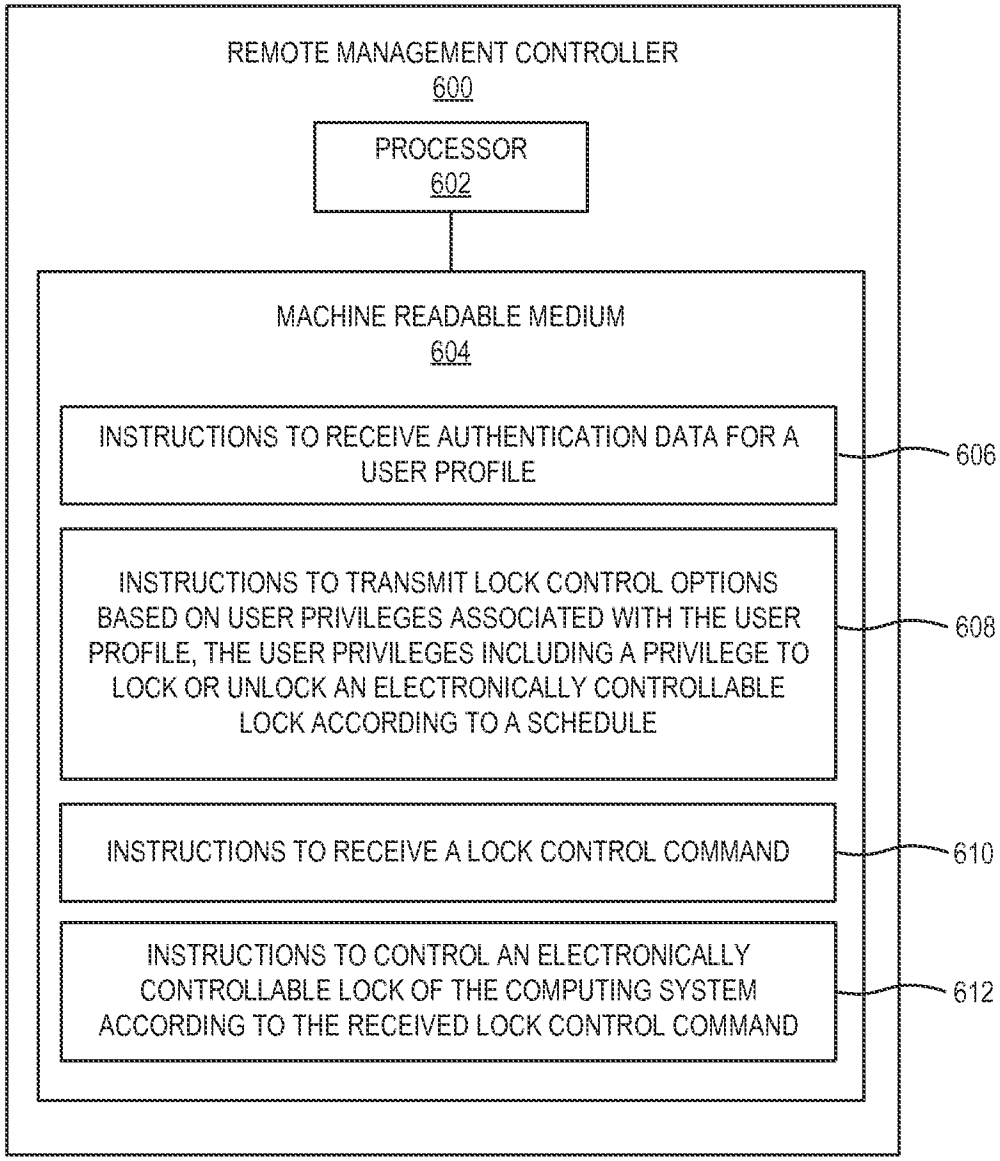
REMOTE MANAGEMENT CONTROLLER
600
PROCESSOR
602
MACHINE READABLE MEDIUM
604
INSTRUCTIONS TO RECEIVE AUTHENTICATION DATA FOR A USER PROFILE
606
INSTRUCTIONS TO TRANSMIT LOCK CONTROL OPTIONS BASED ON USER PRIVILEGES ASSOCIATED WITH THE USER PROFILE, THE USER PRIVILEGES INCLUDING A PRIVILEGE TO LOCK OR UNLOCK AN ELECTRONICALLY CONTROLLABLE LOCK ACCORDING TO A SCHEDULE
608
INSTRUCTIONS TO RECEIVE A LOCK CONTROL COMMAND
610
INSTRUCTIONS TO CONTROL AN ELECTRONICALLY CONTROLLABLE LOCK OF THE COMPUTING SYSTEM ACCORDING TO THE RECEIVED LOCK CONTROL COMMAND
612

FIG. 6

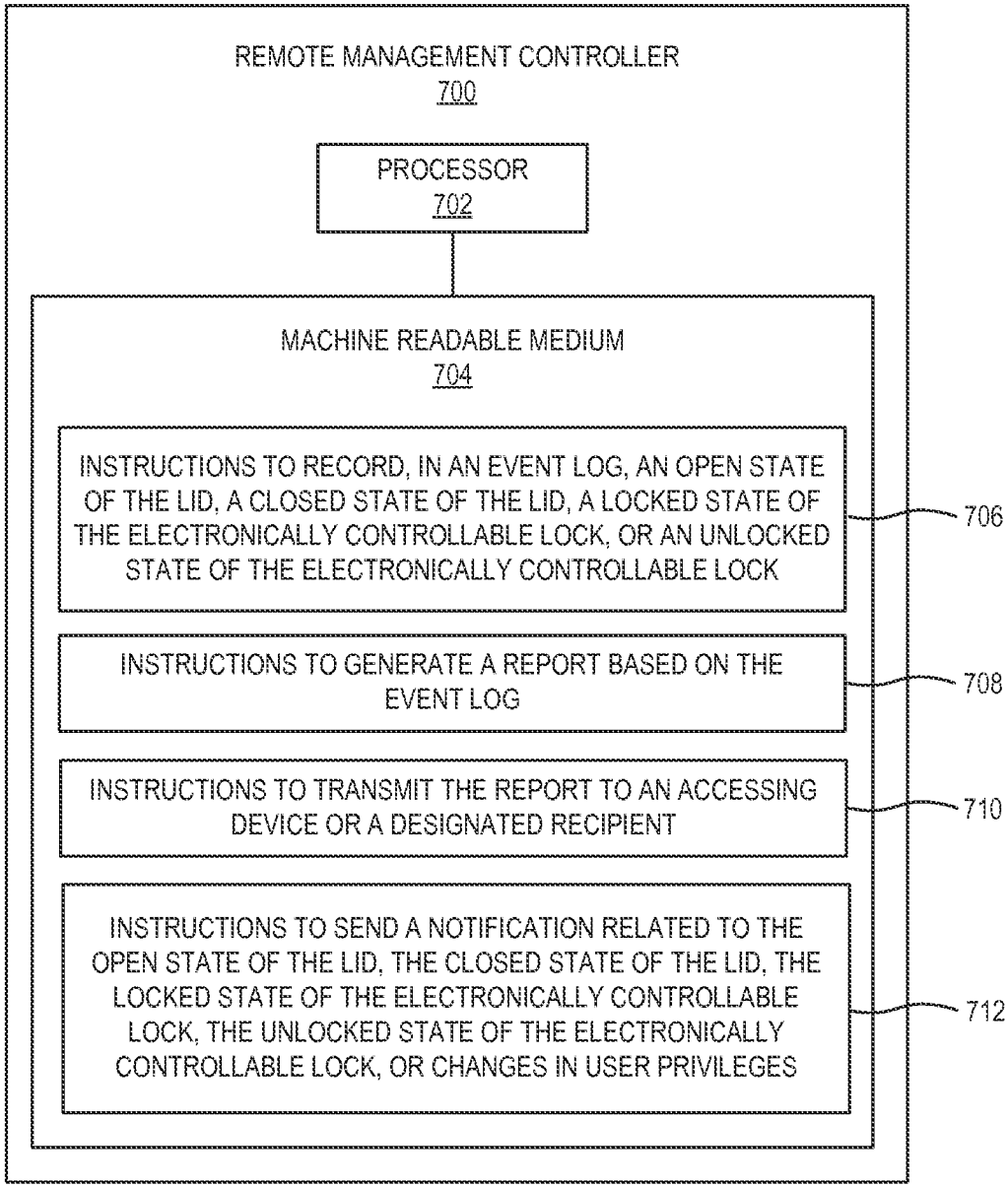
REMOTE MANAGEMENT CONTROLLER
700
PROCESSOR
702
MACHINE READABLE MEDIUM
704
INSTRUCTIONS TO RECORD, IN AN EVENT LOG, AN OPEN STATE OF THE LID, A CLOSED STATE OF THE LID, A LOCKED STATE OF THE ELECTRONICALLY CONTROLLABLE LOCK, OR AN UNLOCKED STATE OF THE ELECTRONICALLY CONTROLLABLE LOCK
706
INSTRUCTIONS TO GENERATE A REPORT BASED ON THE EVENT LOG
708
INSTRUCTIONS TO TRANSMIT THE REPORT TO AN ACCESSING DEVICE OR A DESIGNATED RECIPIENT
710
INSTRUCTIONS TO SEND A NOTIFICATION RELATED TO THE OPEN STATE OF THE LID, THE CLOSED STATE OF THE LID, THE LOCKED STATE OF THE ELECTRONICALLY CONTROLLABLE LOCK, THE UNLOCKED STATE OF THE ELECTRONICALLY CONTROLLABLE LOCK, OR CHANGES IN USER PRIVILEGES
712

FIG. 7

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/US2015/042810**

**A. CLASSIFICATION OF SUBJECT MATTER**

**G06F 21/86(2013.01)i, G06F 21/88(2013.01)i, H05K 7/14(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/86; H05K 7/14; H04L 9/32; G05B 23/02; H05K 5/00; G06F 7/04; G06F 1/16; G06F 21/88

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: electronic lid lock, electronic component lock, remote management controller, lock control command

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 2010-0141379 A1 (PETER T. TUCKER et al.) 10 June 2010<br>See paragraphs [0050]-[0058]; and claims 9, 19. | 1-15 |
| Y | US 2008-0271122 A1 (JOHN EDWARD NOLAN et al.) 30 October 2008<br>See paragraphs [0032]-[0065]; and figures 1D-2D. | 1-15 |
| A | US 2010-0237987 A1 (CONSTANTINE A. BARZACANOS) 23 September 2010<br>See paragraphs [0025]-[0029]; claims 1-10; and figures 7-9. | 1-15 |
| A | US 2014-0146459 A1 (METHODE ELECTRONICS, INC.) 29 May 2014<br>See paragraphs [0048]-[0058]; claim 16; and figures 1-2. | 1-15 |
| A | US 6529382 B2 (MASAYUKI TERAO) 04 March 2003<br>See column 2, line 46 - column 3, line 50; and figures 2A-2B. | 1-15 |

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 05 April 2016 (05.04.2016) | **19 April 2016 (19.04.2016)** |

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Bum
Telephone No. +82-42-481-8398

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.
**PCT/US2015/042810**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2010-0141379 A1 | 10/06/2010 | CN 102239702 A | 09/11/2011 |
| | | DE 112009003517 T5 | 06/06/2012 |
| | | GB 2477651 A | 10/08/2011 |
| | | WO 2010-065807 A1 | 10/06/2010 |
| US 2008-0271122 A1 | 30/10/2008 | None | |
| US 2010-0237987 A1 | 23/09/2010 | US 8581691 B2 | 12/11/2013 |
| US 2014-0146459 A1 | 29/05/2014 | EP 2693856 A2 | 05/02/2014 |
| | | EP 2693856 A3 | 21/05/2014 |
| | | US 2014-0029198 A1 | 30/01/2014 |
| | | US 8854822 B2 | 07/10/2014 |
| | | US 8917512 B2 | 23/12/2014 |
| US 6529382 B2 | 04/03/2003 | JP 03835033 B2 | 18/10/2006 |
| | | JP 2000-194448 A | 14/07/2000 |
| | | JP 2000-195025 A | 14/07/2000 |
| | | US 2002-0075657 A1 | 20/06/2002 |