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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2014 (18.09.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/145962 A2

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/US2014/030822

(22) International Filing Date:
17 March 2014 (17.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/800,496 15 March 2013 (15.03.2013) US

(71) Applicant: **ARDENT SOUND, INC.** [US/US]; 33 South Sycamore Street, Mesa, AZ 85202 (US).

(72) Inventor: **BARTHE, Peter, G.**; 15002 South 30th Street, Phoenix, AZ 85048 (US).

(74) Agent: **LANG, Michael, J.**; Ardent Sound, Inc, 33 South Sycamore Street, Mesa, AZ 85202 (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, LT, 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, 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).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2014/145962 A2

(54) Title: METHODS AND SYSTEMS FOR CONTROLLING MEDICAL DEVICE USAGE

(57) Abstract: Various embodiments provide systems and methods for securely transferring data from a secured site to a medical device. Some embodiments provide systems and methods for securely uploading data from a medical device to a secured site. In some embodiments described herein, data can be downloaded from a secured site to a key and after severing communication with the secured site, key can be coupled to a device and download the data to the device, in some embodiments, a public and private key pair may be used to securely download data to a device.

Title: METHODS AND SYSTEMS FOR CONTROLLING MEDICAL DEVICE USAGE

Inventors: Peter Barthe
Vadim Kouklev

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of US Provisional Patent Application Serial No. 61/800,496, entitled "Methods and Systems for Controlling Medical Device Usage", filed March 15, 2013, which is incorporated by reference herein.

BACKGROUND

[0002] As computerization of medical devices becomes commonplace, such devices may be designed to be interfaced onto a computer network. A networked medical device may allow the device to communicate with a database on the network to transfer data or to upload patient information. However, a networked device can be corrupted via viruses, worms, root-kits, remote access, denial of service, and other malware and attacks, which is important for medical devices. In addition, a non-networked device is simplified and less prone to obsolescence as network technologies and settings change. Regulatory agencies may require a threat analysis and additional testing of a networked medical device.

[0003] In some cases, a personal key can authenticate a user of a computer and then authentication and encryption hardware/firmware, which may be resident on the key, can allow certain usage of hardware and/or software by the computer. In some instances, such usage may be debited or checked from the key before, during, and/or

after the certain usage by the computer is attempted, in process, or completed. The key can protect the operating software on the computer to various degrees against hacker attempts to change it, with the key.

SUMMARY

[0004] Various embodiments provide systems and methods for controlling medical device usage. Some embodiments provide limits of use for a disposable component coupled to a device. For example, a limit of use for disposable component can be a number of treatments that can be performed with the disposable component. Another sample a limit of use for disposable component can be a particular treatment that the device can perform while coupled to disposable component.

[0005] Various embodiments provide systems and methods for securely transferring data from a secured site to a medical device. Some embodiments provide systems and methods for securely uploading data from a medical device to a secured site. In some embodiments described herein, data can be downloaded from a secured site to a key and after severing communication with the secured site, key can be coupled to a device and download the data to the device. In some embodiments, a public and private key pair may be used to securely download data to a device.

[0006] Accordingly, various embodiments provide methods for using a component coupled to a medical device. In some embodiments, a method can include the steps of interfacing a communication key with a computer cloud; downloading encrypted authorization codes from the cloud onto key; severing communication between the cloud and the key; interfacing the key with a device controller in communication with

a medical device; coupling a component to the medical device; downloading the authorization codes to at least one of the medical device and the component; and initiating the component for use when coupled to the medical device.

[0007] Various embodiments provide a treatment system. In some embodiments, the system can include a secured key comprising encrypted protected memory; a secured site located on a computing cloud and configured to securely communicate with the secured key; an interface configured for secured communication between the secured site and the secured key; a treatment device; a device controller in communication with and configured to control the treatment device, the device controller comprising a communication port configured for communication with the secured key; and a component coupled to the treatment device and in communication with the secured key.

[0008] Various embodiments provide methods of enabling a treatment device. In some embodiments, a method can include the steps of downloading an authorization code from a cloud computing network on to a secured electronic key; interfacing the secured electronic key with component treatment module coupled to a treatment device; initiating communication between the secured electronic key and the component treatment module; determining if the component treatment module is enabled to be authorized by the secured electronic key; downloading the authorization code to the component treatment module; authorizing the component treatment module with the authorization code; and enabling operation of the treatment device coupled to the component treatment module, which has been authorized.

DRAWINGS

[0009] The present disclosure will become more fully understood from the specification and the accompanying drawings, wherein:

[0010] FIG. 1 is a diagram illustrating a system, in accordance with various embodiments;

[0011] FIG. 2 is a diagram illustrating a system, in accordance with some embodiments;

[0012] FIG. 3 is a diagram illustrating a system, in accordance with some embodiments;

[0013] FIG. 4 is a diagram illustrating a system, in accordance with some embodiments;

[0014] FIG. 5 is a diagram illustrating a system, in accordance with some embodiments;

[0015] FIG. 6 is a diagram illustrating a system, in accordance with some embodiments;

[0016] FIG. 7 is a diagram illustrating a system, in accordance with some embodiments;

[0017] FIG. 8 is a flowchart illustrating methods, in accordance with some embodiments;

[0018] FIG. 9 is a flowchart illustrating methods, in accordance with some embodiments;

[0019] FIG. 10 is a flowchart illustrating methods, in accordance with some embodiments;

[0020] FIG. 11 is a flowchart illustrating methods, in accordance with some embodiments; and

[0021] FIG. 12 is a flowchart illustrating methods, in accordance with some embodiments.

[0022] The drawings described herein are for illustrative purposes only of selected embodiments and not all possible implementations, and are not intended to limit the scope of any of the exemplary embodiments disclosed herein or any equivalents thereof. It is understood that the drawings are not drawn to scale. For purposes of clarity, the same reference numbers will be used in the drawings to identify similar elements.

DESCRIPTION

[0023] The various embodiments may be described herein in terms of various functional components and processing steps. It should be appreciated that such components and steps may be realized by any number of hardware components configured to perform the specified functions. For example, various embodiments may employ various medical treatment devices, visual imaging and display devices, input terminals and the like, which may carry out a variety of functions under the control of one or more control systems or other control devices. In addition, the embodiments may be practiced in any number of medical contexts and that the various embodiments relating to a method and system for acoustic tissue treatment, as described herein, are merely indicative of exemplary applications for the invention. For example, the principles, features and methods discussed may be applied to any medical application.

[0024] Various embodiments provide systems and methods for controlling medical device usage. Some embodiments provide limits of use for a disposable component coupled to a device. For example, a limit of use for disposable component can be a number of treatments that can be performed with the disposable component. In another example, a limit of use for disposable component can be a particular treatment that the device can perform while coupled to disposable component.

[0025] Various embodiments provide systems and methods for securely transferring data from a secured site to a medical device. Some embodiments provide systems and methods for securely uploading data from a medical device to a secured site. In some embodiments described herein, data can be downloaded from a secured site to a key and after severing communication with the secured site, key can be coupled to a

device and download the data to the device. In some embodiments, a public and private key pair may be used to securely download data to a device.

[0026] In various embodiments, data can be any type of data that can be downloaded from a secured site to a device. The data can be a data packet that is downloadable from the secured site to the device. For example, data can allow and/or limit usage of the device, such as for example, a medical device. In another example, data can be a device upgrade, for example, a software upgrade, or a new software module or a new version of software. For example, data can be a new method, such as for example a new treatment method for medical device. In another example data can be an activation of option, when the option resides on the device but is dormant.

[0027] In another example, data can be a lifetime of a particular component. A lifetime can be a number of treatments that can be performed with the disposable component. A lifetime of a particular component can be for example a prescribed number of lines available for an emission source. For example, an emission source can be at least one of an ultrasound transducer, a RF generator, and a laser. In one example, an emission source is an ultrasound transducer.

[0028] Various embodiments provide a treatment system. In some embodiments, the system can include a secured key comprising encrypted protected memory; a secured site located on a computing cloud and configured to securely communicate with the secured key; an interface configured for secured communication between the secured site and the secured key; a treatment device; a device controller in communication with and configured to control the treatment device, the device controller comprising a communication port configured for communication with the secured key; and a

component coupled to the treatment device and in communication with the secured key.

[0029] In some embodiments, the system can include a processor configured to communicate with the secured site and comprising a communication port configured for communication with the secured key. In some embodiments, the treatment device is an ultrasound treatment device. In some embodiments, the component is an ultrasound transducer module. In some embodiments, the component comprises an EEPROM configured to communicate with the secured key and comprising an authorization protocol.

[0030] In some embodiments, the system can include an authorization code configured to be downloaded from the secured site onto the secured key and further configured to be transmitted from the secured key to the EEPROM. In some embodiments, the authorization code is configured to be delivered to the authorization protocol and permit the authorization protocol to enable operation of the component. In some embodiments, the system can include a treatment counter embedded into the secured key and in communication with the component.

[0031] In some embodiments, the system can include an expiration function configured to execute after a predetermined number of treatments as clocked by the treatment counter and configured disable operation of the component upon completion of the predetermined number of treatments. In some embodiments, the treatment device, the device controller and the communication port are enclosed into one unit.

[0032] In some embodiments, the system can include an interface sever module configured to sever the interface between the secured server and the secured key and configured

to automatically sever the interface upon communication of the device controller with the secured key. In some embodiments, the system can include a software update configured to be delivered from the secured site to the secured key and further configured to be uploaded from the secured key to the device controller and configured to update the software rev on running the device controller. In some embodiments, the system can include a firewall configured to automatically operate upon operation of the component and configured to prevent any communication to the device controller with the cloud.

[0033] Now with reference to FIG. 1, a diagram illustrating a system is presented in accordance with various embodiments. System 100 comprises a key 101 which can be configured to interface with a processor 107 as well as, with a controller 110. Processor 107 communicates with cloud 105 through an interface 106. Controller 110 communicates with a device 114. In some embodiments, device 114 comprises controller 110. In some embodiments, device 114 comprises memory, which is in communication with controller 110. Controller 110 communicates with and controls device 114.

[0034] In various embodiments, cloud 105 can be any system or network that enables processor 107 to communicate with a control site which may be a webpage or may be located on a secure server. In some embodiments, cloud 105 can be the Internet. For example, cloud 105 enables processor 107 to communicate via interface 106 with a secured website. In some embodiments, processor 107 can communicate with cloud 105 using a web browser. In some embodiments, processor 107 can communicate with cloud 105 using an app, which may be installed on processor 107.

[0035] Processor 107 can be a computer, such as, for example a desktop, a lap top, or notebook. In some embodiments, processor 107 can be a computer configured with the wired port for use as interface 106 for communication with cloud 105. In some embodiments, processor 107 can be a computer configured with a wireless port for use as interface 106 for communication with the cloud 105. In some embodiments, processor 107 can be a computer configured with both a wired port and a wireless port, either or both being configured for use as interface 106 for communication with the cloud 105. In some embodiments, processor 107 can be a smart device, such as for example, a tablet, a smart phone, an iPhone, an iPad, or a PDA. Interface 106 can be based on an Ethernet system, a wireless system, a LAN, a WAN, a cellular system, a radio system, or combinations thereof.

[0036] Processor 107 can be any device which can communicate with cloud 105 and comprises a port which can allow key 101 to communicate with processor 107, which can allow cloud 105 to communicate with key 101. In some embodiments, processor 107 comprises a port which is a USB interface to which key 101 is configured to couple to such a port. In some embodiments, processor 107 comprises a port which physically and electronically couples with key 101. In some embodiments, processor 107 comprises a wireless port which communicates wirelessly with key 101. In some embodiments, the port is configured to communicate with key 101 and allow key 101 to couple to processor 107.

[0037] Various embodiments provide methods for employing key 101 for use with device 114. Some embodiments provide methods for controlling usage of device 114. In some embodiments, device 114 can be a medical device. Processor 107 can be

connected with cloud 105 via interface 106, which allows communication with the secured website hosted in cloud 105. After security authorization is recognized by the website, key 101 is interfaced with processor 107 (as indicated by arrow "1"). Processor 107 can facilitate a data upload from key 101 to the website. Processor 107 can facilitate a data download from the website onto key 101. For example, processor 107 can provide data to website and this data can be used to determine if device 110 is valid. After website has gone through a process to determine the validity of device 114, website sends authorization codes through processor 107 to key 101. After authorization codes have been received and confirmed by key 101, the interface between key 101 and processor 107 is severed. In some embodiments, after authorization codes have been received and confirmed by key 101, the interface between key 101 and cloud 105 is severed. Although the interface between key 101 and processor 107 is severed, processor 107 may still be in communication with cloud 105 via interface 106.

[0038] Since interface between key 101 and processor 107 has been severed, key 101 can be interfaced with controller 110 (as indicated by arrow labeled "2"). In various embodiments, key 101 can be used to authenticate device 114. In some embodiments, controller 110 comprises a port that is equivalent to the port of processor 107. In some embodiments, controller comprises a wireless port configured to be in communication with key 101. Although port of controller 110 may not be equivalent on to port of processor 107, port of controller 110 is configured to allow key 101 to be in communication with device 114. In some embodiments, controller 110 is configured to allow key 101 to be in communication with device 114.

Controller 110 can facilitate a data upload from key 101 to the device 114. Controller can facilitate a data download from the device 114 onto key 101.

[0039] Now with reference to FIG. 2, a diagram illustrating a system is presented in accordance with various embodiments. System 100 comprises key 101 which can be configured to interface with processor 107 as well as, with controller 110. Processor 107 communicates with cloud 105 through an interface 106. Device 114 comprises controller 110. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. Controller 110 communicates with and controls both device 114 and component 115. In some embodiments, device 114 comprises memory, which is in communication with controller 110.

[0040] Various embodiments provide methods for employing key 101 for use with device 114 and component 115. Processor 107 can be connected with cloud 105 via interface 106, which allows communication with a website hosted in cloud 105. After security authorization is recognized by the website, key 101 is interfaced with processor 107 (as indicated by arrow "1"). Processor 107 can facilitate a data upload from key 101 to the website. Processor 107 can facilitate a data download from the website onto key 101. After data has been uploaded onto key 101, the interface between key 101 and processor 107 is severed.

[0041] Since interface between key 101 and processor 107 has been severed, key 101 can be interfaced with controller 110 (as indicated by arrow labeled "2"). In various embodiments, key 101 can be used to download data onto device 114 and/or component 115. For example, key 101 can be used to authenticate component 115. In

another example, key 101 can be used to authenticate both device 114 and component 115. In some embodiments, controller 110 is configured to allow key 101 to be in communication with component 115. In some embodiments, controller 110 is configured to allow key 101 to be in communication with both device 114 and component 115.

[0042] In various embodiments, component 115 is coupled to device 114 (as indicated by arrow "3"). In some embodiments, key 101 contains data configured to enable component 115 for operation, key 101 is coupled to the controller 110, which is enabled for communication with at least one of device 114 and component 115. When device 114 is operated, key 101 provides data, such as for example, authorization codes, to allow component 115 to function when coupled to device 114. In various embodiments, controller 110 facilitates a data upload from component 115.

[0043] Now with reference to FIG. 3, a diagram illustrating a system is presented in accordance with various embodiments. System 100 comprises a key 101 which can be configured to interface with a processor 107 as well as, with a controller 110. Processor 107 communicates with cloud 105 through an interface 106. Controller 110 communicates with a device 114 through a device interface 113. In some embodiments, controller 110 communicates with and controls device 114. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. In some embodiments, controller 110 communicates with and controls both device 114 and component 115. In some embodiments, device 114 comprises memory, which is in communication with controller 110.

[0044] In various embodiments, component 115 is coupled to device 114 (as indicated by arrow "3"). In some embodiments, key 101 contains data configured to enable component 115 for operation, key 101 is coupled to the controller 110, which is enabled for communication with at least one of device 114 and component 115. When device 114 is operated, key 101 provides data, such as for example, authorization codes, to allow component 115 to function when coupled to device 114. In various embodiments, controller 110 facilitates a data upload from component 115. In one example, key 101 uploads data that tracks the use of component 115. In one example, component 115 has a prescribed lifetime, which is based on a number of treatments and such predetermined number of treatments can be downloaded as data to key 101 from the website. Upon an expiration of the lifetime of the component 115, key 101 terminates activation of the data, such as, for example, authorization codes, which was sent to device 114 and/or component 115, thus making device 114 inoperable.

[0045] In one example, upon an expiration of the lifetime of the component, key 101 invalidates the data that was sent to component 115, thus making component 115 inoperable. In one example, upon an expiration of the lifetime of the component 115, key 101 removes the data that was sent to device 114, thus making at least one of device 114 and component 115 inoperable. In an example, upon an expiration of the lifetime of the component 114, key 101 terminates data being sent to component 115, thus making component 115 inoperable. In an example, upon an expiration of the finite lifetime of the component, key 101 invalidates data, such as, for example, authorization codes, sent to both device 114 and component 115, thus making device 114 and component 115 inoperable. In one example, interface between key 101 and

controller 110 is can be severed and key 101 is then interfaced with cloud 115, to download data to key 101, such as, for example, additional lifetime and the corresponding new authorization codes, which can be downloaded to at least one of the device 114 and component 115.

[0046] Now with reference to FIG. 3, a diagram illustrating a system is presented in accordance with various embodiments. System 100 comprises key 101 which can be configured to interface with processor 107 as well as, with controller 110. Processor 107 communicates with cloud 105 through an interface 106. Controller 110 communicates with a device 114 through a device interface 113. In some embodiments, controller 110 communicates with and controls device 114. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. In some embodiments, controller 110 communicates with and controls both device 114 and component 115. In some embodiments, device 114 comprises memory, which is in communication with controller 110.

[0047] Moving to FIG 4, a diagram illustrating a system is presented in accordance with various embodiments. System 1100 comprises key 101 which can interface with cloud 105 through an interface 106, as well as, with controller 110. Device 114 comprises controller 110. In some embodiments, controller 110 communicates with and controls device 114. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. In some embodiments, controller 110 communicates with and controls both device 114 and component 115. In some embodiments, device 114 comprises memory, which is in communication with controller 110.

[0048] In various embodiments, cloud 105 can be any system or network that enables key 101 to communicate with a control site which may be a webpage or may be located on a secure server. In some embodiments, cloud 105 can be the Internet. For example, cloud 105 enables key 101 to communicate via interface 106 with a secured website. In some embodiments, key 101 can communicate with cloud 105 using a web browser. In some embodiments, key 101can communicate with cloud 105 using an app, which may be installed on key 101.

[0049] Various embodiments provide methods for employing key 101 for use with device 114. Key 101 can be connected with cloud 105 via interface 106, which allows communication with a website hosted in cloud 105. In some embodiments, website goes through a process to determine the validity of component 115, and website then sends data to key 101. "). Interface 106 can facilitate a data upload from key 101 to the website. Interface 106 can facilitate a data download from the website onto key 101. After data has been uploaded onto key 101, the interface between key 101 and processor 107 is severed. After data has been received and confirmed by key 101, the interface between key 101 and cloud 105 is severed.

[0050] Since interface between key 101 and cloud 105 has been severed, key 101 can be interfaced with controller 110 (as indicated by arrow labeled "1"). In various embodiments, key 101 can be used to authenticate device 114 and/or component 115. In various embodiments, key 101 can be used to authenticate component 115. In various embodiments, key 101 can be used to authenticate device 114. In various embodiments, key 101 can be used to authenticate both device 114 and component 115. In some embodiments, controller comprises a wireless port configured to be in

communication with key 101. Although port of controller 110 may not be equivalent on to port of processor 107, port of controller 110 is configured to allow key 101 to be in communication with device 114 and/or component 115. In some embodiments, controller 110 is configured to allow key 101 to be in communication with device 114. In some embodiments, controller 110 is configured to allow key 101 to be in communication with component 115. In some embodiments, controller 110 is configured to allow key 101 to be in communication with both device 114 and component 115.

[0051] In various embodiments, component 115 is coupled to device 114 (as indicated by arrow "3"). In some embodiments, key 101 contains data configured to enable component 115 for operation, key 101 is coupled to the controller 110, which is enabled for communication with at least one of device 114 and component 115. When device 114 is operated, key 101 provides data, such as for example, authorization codes, to allow component 115 to function when coupled to device 114. In various embodiments, controller 110 facilitates a data upload from component 115. In one example, key 101 uploads data that tracks the use of component 115. In one example, component 115 has a prescribed lifetime, which is based on a number of treatments and such predetermined number of treatments can be downloaded as data to key 101 from the website. Upon an expiration of the lifetime of the component 115, key 101 terminates activation of the data, such as, for example, authorization codes, which was sent to device 114 and/or component 115, thus making device 114 inoperable. Is one example, upon an expiration of the lifetime of the component, key 101 invalidates the data that was sent to component 115, thus making component 115

inoperable. In one example, upon an expiration of the lifetime of the component 115, key 101 removes the data that was sent to device 114, thus making at least one of device 114 and component 115 inoperable. In an example, upon an expiration of the lifetime of the component 114, key 101 terminates data being sent to component 115, thus making component 115 inoperable. In an example, upon an expiration of the finite lifetime of the component, key 101 invalidates data, such as, for example, authorization codes, sent to both device 114 and component 115, thus making device 114 and component 115 inoperable. In one example, interface between key 101 and controller 110 is can be severed and key 101 is then interfaced with cloud 115, to download data to key 101, such as, for example, additional lifetime and the corresponding new authorization codes, which can be downloaded to at least one of the device 114 and component 115.

[0052] Moving to FIG 5, a diagram illustrating a system is presented in accordance with various embodiments. System 1100 comprises key 101 which could interface with cloud 105 through an interface 106, as well as, with controller 110. Controller 110 communicates with device 114 through a device interface 113. In some embodiments, controller 110 communicates with and controls device 114. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. In some embodiments, controller 110 communicates with and controls both device 114 and component 115. In some embodiments, device 114 comprises memory, which is in communication with controller 110.

[0053] Turning to FIG 6, a diagram illustrating a system is presented in accordance with various embodiments. System 1200 comprises controller 110, which can interface

with cloud 105 through an interface 106. Device 114 comprises controller 110. In some embodiments, controller 110 communicates with and controls device 114. In some embodiments, device 114 comprises memory, which is in communication with controller 110. In some embodiments, secured site 150 can include a secured interface 155 through cloud 105. For example, secured interface 155 can be a VPN.

[0054] In FIG 7, a diagram illustrating a system is presented in accordance with various embodiments. System 1200 comprises controller 110, which could interface with cloud 105 though interface 106. Controller 110 communicates with device 114 through a device interface 113. In some embodiments, controller 110 communicates with and controls device 114. In various embodiments, device 114 comprises a component 115, which can be coupled to and uncoupled from device 114. In some embodiments, controller 110 communicates with and controls both device 114 and component 115. In some embodiments, component 115 communicates with cloud 105 though interface 156. In some embodiments, secured site 150 can include a secured interface 155 through cloud 105. For example, secured interface 155 can be a VPN.

[0055] With reference back to FIGS. 1-5, various embodiments provide methods for employing key 101 for use with device 114. Some embodiments provide methods for controlling usage of device 114. In some embodiments, device 114 can be a medical device. Processor 107 can be connected with cloud 105 via interface 106, which allows communication with a website hosted in cloud 105. After security authorization is recognized by the website, key 101 is interfaced with processor 107 (as indicated by arrow "1"). Processor 107 can provide data to website and this data

can be used to determine if component 115 is valid. After website has gone through a process to determine the validity of component 115, website sends authorization codes through processor 107 to key 101. After authorization codes have been received and confirmed by key 101, the interface between key 101 and processor 107 is severed. In some embodiments, after authorization codes have been received and confirmed by key 101, the interface between key 101 and cloud 105 is severed. Although the interface between key 101 and processor 107 is severed, processor 107 may still be in communication with cloud 105 via interface 106.

[0056] Various embodiments provide methods for using a component coupled to a medical device. In some embodiments, a method can include the steps of interfacing a communication key with a computer cloud; downloading encrypted authorization codes from the cloud onto key; severing communication between the cloud and the key; interfacing the key with a device controller in communication with a medical device; coupling a component to the medical device; downloading the authorization codes to at least one of the medical device and the component; and initiating the component for use when coupled to the medical device.

[0057] In some embodiments, a method can include the step of determining if the component is valid. In some embodiments, a method can include the step of operating the medical device and the component.

[0058] In some embodiments, the method can include the step of counting a number of treatments performed by the component during the operating the medical device and the component. In some embodiments, the method can include the step of providing a limit of the number of treatments performed by the component during the operating

the medical device and the component. In some embodiments, the method can include the step of disabling the component upon reaching the limit of the number of treatments performed by the component during the operating the medical device and the component.

[0059] In some embodiments, the authorization codes enable operation of the component. In some embodiments, the method can include the step of reviewing a current version of software on the controller. In some embodiments, the method can include the step of determining if a software update is available on the key. In some embodiments, the method can include the step of downloading the software update to the controller and updating the current software with the software update.

[0060] Various embodiments provide methods of enabling a treatment device. In some embodiments, a method can include the steps of downloading an authorization code from a cloud computing network on to a secured electronic key; interfacing the secured electronic key with component treatment module coupled to a treatment device; initiating communication between the secured electronic key and the component treatment module; determining if the component treatment module is enabled to be authorized by the secured electronic key; downloading the authorization code to the component treatment module; authorizing the component treatment module with the authorization code; and enabling operation of the treatment device coupled to the component treatment module, which has been authorized.

[0061] In some embodiments, a method can include the steps of disabling the component treatment module, if the component treatment module is not enabled to be authorized

by the secured electronic key; and preventing operation of the treatment device coupled to the component treatment module, which has been disabled.

[0062] In some embodiments, a method can include operating the treatment device coupled to the component treatment module, which has been authorized. In some embodiments, a method can include counting on the secured electronic key a number of treatments performed by the component treatment module during the operating the treatment device coupled to the component treatment module, which has been authorized. In some embodiments, a method can include providing on the secured electronic key a limit of the number of treatments performed by the component treatment module during the operating the treatment device coupled to the component treatment module, which has been authorized. In some embodiments, a method can include disabling the component treatment module upon reaching the limit of the number of treatments performed by the component during the operating the treatment device coupled to the component treatment module, which has been authorized.

[0063] In some embodiments, a method can include establishing a communication interface between the secured electronic key and the cloud computing network before the step of downloading the authorization code from the cloud computing network on to the secured electronic key. In some embodiments, a method can include severing the communication interface between the secured electronic key and the cloud computing network after the step of downloading the authorization code from the cloud computing network on to the secured electronic key.

[0064] In some embodiments, a method can include the steps of downloading a software update from the cloud computing network onto the secured electronic key; notifying

the treatment device of the software update upon the step of the initiating communication between the secured electronic key and the component treatment module; downloading the software update from the secured electronic key to the treatment device; and initiating the software update on the treatment device.

[0065] In some embodiments, a method can include preventing the secured electronic key from interfacing with the cloud computing network upon the step of the initiating communication between the secured electronic key and the component treatment module. In some embodiments, a method can include delivering the authorization code to the secured electronic key from an attachment to an email message. In some embodiments, the treatment device and the secured electronic key integrated together into a single device.

[0066]

[0067] Examples

[0068] Moving to FIG 8, a flowchart illustrating operation of the system is provided, according to various embodiments. According to various methods, a user wants to acquire asset(s) (step 401), which is configured for link to secured site (step 402). In one example, link to site 402 can be a user coupling key 101 to processor 107. In another example, the secured site may be located at factory or at a vendor or distributor location.

[0069] In various embodiments, asset(s) can be any type of data that can be transferred from a secured site to the user. Asset(s) a data packet that is downloadable from the secured site to the user. For example, asset can be allowed usage of the device, such as for example, a medical device. In another example, asset can be a system upgrade,

for example, a software upgrade, or a new software module or a new version of software. For example, asset can be a new method, such as for example a new treatment method for medical device. In another example asset can be an activation of assistant option, when the option resides on the device but is dormant. In another example, asset can be a lifetime of a particular component. A lifetime of a particular component can be for example a prescribed number of lines available for an emission source. For example, an emission source can be at least one of an ultrasound transducer, a RF generator, and a laser. In one example, an emission source is an ultrasound transducer.

[0070] Once link to site 402 has been completed, site authenticates user (step 403). In one example, site authenticates user (step 403) can be a server at a secure site reads key 101. After site authenticates user (step 403), a set of assets are listed (step 405). In one example, a set of assets are listed (step 405) can be the server and the secure site returns a listing of assets that can be read on a display of processor 107. In the next step, user enters chosen assets (step 406) and optionally secured site loads chosen assets (step 407). In one example, user enters chosen assets (step 406) can be a user entering a selection of assets into processor 107. In one example, secured site loads chosen assets (step 407) can be the secured site downloading data to key 101 via processor 107. The methods continue with site enables chosen assets (step 408). In one example, the chosen assets may reside on key 101 and secured site downloads authentication codes to key 101, which allow chosen assets to be operational and access to the chosen assets given the user. Finally, user employs asset (step 409).

[0071] Optional step can be upload user data to secured site (step 410). For example, user data can be user logs generated by the device, which employs at least one of the chosen assets. In one example, user data can be diagnostic information useful in troubleshooting the device, which employs at least one of the chosen assets. One example, user data can be device usage information. In some embodiments, user data can be any information that can be downloaded from the users device to the secured site. In some embodiments, user data is downloaded to key 101 which is coupled to users device, then key 101 can download user data to secured site. One example, key 101 which contains downloaded user data, can be coupled to processor 107, which can facilitate an interface between key 101 and the secured site, in order to, transfer the downloaded user data from key 101 to the secured site.

[0072] Referring to FIG 9, a flowchart illustrating operation of the system is provided, according to various embodiments. A method can begin with factory generating and storing a private and public key pair (step 501). The next step is write public key into device (step 502) and ship device to user (step 503). After receiving device, user uses device (step 504). Next is a decision in which user or factory solicits change to device (step 505). If no (506), use of the device continues looping back to user uses device (step 505). If yes (507), the next step is user links to site (step 508), followed by site authenticates device via device keys (step 509). In one example, site is located at factory. In another example, site is located at distributor and private and public key pair has been transferred to distributor. Still another example, the site is located at factory and one or more sites are located at one or more distributors which have access to the private and public key pair.

[0073] After site authenticates device via device keys (step 509), site recalls private key (step 510). Site generates data for the change and then site encrypts data with private key (step 511). Site sends encrypted data to device (step 513). Upon receipt of the encrypted data, device decrypts data with its public key and validates data digital signature (step 514). Next is a decision, is signature valid? (step 516). If yes (step 517), user can incorporate data into device then user uses device (step 504). If no (step 518), then loop back to user links to site (step 508). Alternatively, if no (step 518), then the device use is locked (step 520). The device maybe locked (step 520) immediately for no in decision, is signature valid? (step 516). However, the device maybe locked (step 520) after a specified numbers of loop back to user links to site (step 508) and receiving no in decision, is signature valid? (step 516).

[0074] Now with reference to FIG 10, a flowchart illustrating operation of a system is provided, according to various embodiments. FIG 10 is divided into three sections and each section is marked at the top of the figure with the following: 105 which is the domain of cloud 105; 107 which is the domain of processor 107; and 110 which is the domain of controller 110. Each of the operations and/or processes which are indicated on the flowchart will reside in one of the three sections or domains which are one of 101, 107, or 110. For example, if an operation is in the section under the heading of 105, this operation is being performed in cloud 105. In another example, if an operation is in the section under the heading of 107, this operation is being performed by processor 107. Still another example, if an operation is set in the section under heading 110, this operation is being performed by controller 110.

[0075] In the first step, processor 107 connects to a secured site located in cloud 105 (step 201). The secured site in cloud 105 communicates with processor 107 (step 202). Step 201 and step 202 create interface 106. Key 101 is interfaced with processor 107 (step 204). The secured site receives data from key 101 (step 206). The secured site determines if key 101 is valid (step 208). If key 101 is valid then YES (step 212). If key 101 is not valid then NO (step 209) and process ends (step 211). If process ends (step 211), the secured site can send a message to processor 107 communicating status of key 101, as well as, presenting possible remedies to revalidate key 101.

[0076] If YES (step 212), then data from component 115 is entered into processor 107. The data from component 115 may include serial number, user ID, password, and combinations thereof and the like. In addition, other data such as, for example, device 114 serial number, application ID, device location and combinations thereof and the like, maybe entered. The data from component 115 can be entered via a keyboard. In some embodiments, the data from component 115 can be entered by scanning a bar code. In some embodiments, the data from component 115 can be entered via a RFID located in the device which can be read by key 101 or processor 107.

[0077] The secured site, as described herein and which is located in cloud 105 receives the data from component 115 from processor 107 (step 215). The secured site determines if component 115 is valid (step 216). If component 115 is valid then YES (step 230). If component 115 is not valid then NO (step 218) and process ends (step 219). If process ends (step 219), the secured site can send a message to processor 107 communicating status of component 115, as well as, presenting possible remedies to

revalidate component 115. Optionally, if component 115 is not valid then NO (step 222), the secured site offers the purchase of additional component lifetime (step 224). If YES (step 225), additional component lifetime is added and this new component data is received (step 215) by secured site. If NO (step 226) and process ends (step 227). If process ends (step 227), the secured site can send a message to processor 107 communicating status of component 115.

[0078] If component 115 is valid then YES (step 230). The secured site provides authorization codes (step 231) for component 115. The authorization codes are downloaded to key 101 (step 231). The data and/or information related to the component 115, which has been authorized is updated in the database (step 235) of secured site. The interface between key 101 and cloud 105 ends or is severed (step 234).

[0079] Key 101 is then interfaced to controller 110 (step 251). Component 115 is coupled to device 114, which is in communication with controller 110 (step 252). Key 101 determines if component 115 is able to be authorized (step 254). If NO (step 255), and process ends (step 256). If process ends (step 256), key 101 can send a message to processor 107 communicating status of component 115, as well as, presenting a reason for failure, for example, mismatch of component 115 serial numbers. In some embodiments, key 101 communicates with EEPROM on component 115 to determine if component 115 is able to be authorized (step 254). If YES (step 258) then key 101 authorizes component 115 and device 114 can be operated (step 262). In some embodiments, key 101 sends authorization codes to EPPROM in component 115 to enable authorization of component 115.

[0080] In some embodiments, key 101 counts the use of component 115 (step 262). For example, key 101 can be configured to count each run that component 115 has been used. In an example, key 101 can be configured to count each treatment that component 115 has performed. In some embodiments, a finite lifetime of component 115 can be downloaded to key 101. For example, a finite lifetime of component 115 is a predetermined number of treatments performed and after the predetermined number treatments performed is reached, as counted on key 101, the finite lifetime of component 115 expires. In some embodiments, when the finite lifetime of component 115 expires, component 115 is no longer operable. In some embodiments, when the finite lifetime of component 115 expires, device 114 cannot operate when coupled to component 115 with an expired lifetime. Key 101 determines if finite lifetime of component 115 is expired (step 266). If NO (step 267), then device 114 can continue to operate (step 260). If Yes (step 268), then process ends (step 269) and device 114 can no longer operate.

[0081] Optionally, if YES (step 270), then additional lifetime can be added to component 115. If YES (step 270), then the interface between key 101 and controller 110 is ended or severed (step 272). Key 101 is then interfaced with processor 107 (step 273). Processor 107 is interfaced with cloud 105 and the secured site offers the purchase of additional component lifetime (step 224). If YES (step 225), additional component 115 lifetime is added and this new component data is received (step 215) by secured site and the process continues from this step, as previously described.

[0082] In some embodiments, after secured site receives data from key 101 (step 206), secured site determines if a new software rev is available for controller 110 (step

242). If NO (step 243), then this portion of the process ends (step 244). If YES (step 246), then new software rev is downloaded to key (step 248) before the interface between key 101 and cloud 105 ends or is severed (step 234).

[0083] In some embodiments, after secured site receives data from component 115 (step 215), secured site determines if a new software rev is available for device 114 (step 242). If NO (step 243), then this portion of the process ends (step 244). If YES (step 246), then new software rev is downloaded to key (step 248) before the interface between key 101 and cloud 105 ends or is severed (step 234).

[0084] In some embodiments, after key 101 is interfaced to controller 110 (step 251), controller 110 determines if key 101 contains a new software rev (step 281). If NO (step 282), then this portion of the process ends (step 283). If NO (step 282), controller 110 can communicate that software is up to date. If YES (step 287), then controller 110 software is updated from key 101 (step 288). In some embodiments, controller 110 determines if key contains new software rev for device 114 (step 281). If NO (step 282), then this portion of the process ends (step 283). If NO (step 282), controller 110 can communicate that software is up to date. If YES (step 287), then controller 110 updates device 114 software from key 101 (step 288).

[0085] Moving to FIG 11, a flowchart illustrating operation of system 100 is provided according to various embodiments. As illustrated in FIG 10, FIG 11 is also divided into three sections and each section is marked at the top of the figure with the following: 105 which is the domain of cloud 105; 107 which is the domain of processor 107; and 110 which is the domain of controller 110.

[0086] In the first step, data is sent from cloud 105 to processer 107 (step 301). This step can be wireless, using a radio system, such as a GSM system or other cellular based system to which processor 107 can be in communication with. This step can be as simple as sending an email with an attachment to processor 107. In some embodiments, this step can employ text message and the delivery of data through cloud 105 via such a text system. The next step is the data is received by processor 107 (step 302).

[0087] Key 101 is interfaced with processor 107 (step 204). In some embodiments, processor 107 comprises a port which is a USB interface to which key 101 is configured to couple to. In some embodiments, processor 107 comprises a port which communicates wirelessly with key 101. In some embodiments, the port should be configured to communicate with key 101 and allow key 101 to couple to processor 107. The data, which originated in cloud 301, is downloaded to key 101 (step 304).

[0088] In some embodiments, processer 107 determines if key 101 is valid. If key 101 is valid then the data is downloaded. If key 101 is not valid then process ends. If process ends, a message can be transmitted by processor 107 communicating status of key 101, as well as, presenting possible remedies to revalidate key 101. In some embodiments, if process ends, processor 107 can send a message to cloud 105 to update a database of key identification and validation information. After the data is downloaded to key 101, the interface between key 101 and processor 107 is severed.

[0089] Key 101 is then interfaced to controller 110 (step 251). Component 115 is coupled to device 114, which is in communication with controller 110 (step 252). Key 101 determines if component 115 is able to be authorized (step 254). If NO (step 255),

and process ends (step 256). If process ends (step 256), key 101 can send a message to processor 107 communicating status of component 115, as well as, presenting reason for failure, for example, mismatch of component 115 serial numbers. In some embodiments, key 101 communicates with EEPROM on component 115 to determine if component 115 is able to be authorized (step 254). If YES (step 258) then key 101 authorizes component 115 and device 114 can be operated (step 262). In some embodiments, key 101 sends authorization codes to EPPROM in component 115 to enable authorization of component 115.

[0090] In some embodiments, key 101 counts the use of component 115, as illustrated in FIG 11 and as described herein. In some embodiments, after secured site receives data from key 101, secured site determines if a new software rev is available for controller, as illustrated in FIG 11 and as described herein. In some embodiments, after secured site receives data from component 115, secured site determines if a new software rev is available for device 114, as illustrated in FIG 11 and as described herein. In some embodiments, after key 101 is interfaced to controller 110, controller 110 determines if key 101 contains a new software rev, as illustrated in FIG 11 and as described herein.

[0091] Turning to FIG 12, a flowchart illustrating operation of system 100 is provided according to various embodiments. FIG 12 is divided into three sections and each section is marked at the top of the figure with the following: 105 which is the domain of cloud 105; 101 which is the domain of key 101; and 110 which is the domain of controller 110.

[0092] As described in a similar fashion for the flowcharts illustrated in FIG 10 and FIG 11, key 101 connects to cloud 105 (step 350). Cloud 105 communicates with key 101 (step 352), which can be one way or two way communication. Cloud 105 query key 101 (step 354). Decision "any updates?" (step 361). If YES (step 361) cloud collects and sends updates and any other data to key (step 363). Then the key 101 is updated (step 365) and key 101 ends connection to cloud 105 (step 367). If NO (step 362) then key 101 ends connection to cloud 105 (step 367).

[0093] In some embodiments, key 101 counts the use of component 115, as illustrated in FIG 12 and as described herein. In some embodiments, after secured site receives data from key 101, secured site determines if a new software rev is available for controller, as illustrated in FIG 12 and as described herein. In some embodiments, after secured site receives data from component 115, secured site determines if a new software rev is available for device 114, as illustrated in FIG 12 and as described herein.

[0094] In some embodiments, after key 101 is interfaced to controller 110, controller 110 determines if key 101 contains a new software rev, as illustrated in FIG 12 and as described herein.

[0095] As used herein, the terms "comprise", "comprises", "comprising", "having", "including", "includes" or any variation thereof, are intended to reference a non-exclusive inclusion, such that a process, method, device, system, composition or apparatus that comprises a list of elements does not include only those elements recited, but may also include other elements not expressly listed or inherent to such process, method, device, system, composition or apparatus.

[0096] As used herein, the phrase "at least one of A, B, and C" can be construed to mean a logical (A or B or C), using a non-exclusive logical "or," however, can be contrasted to mean (A, B, and C), in addition, can be construed to mean (A and B) or (A and C) or (B and C). As used herein, the phrase "A, B and/or C" should be construed to mean (A, B, and C) or alternatively (A or B or C), using a non-exclusive logical "or."

[0097] It should be understood that steps within a method may be executed in different order without altering the principles of the present disclosure. The some embodiments may be described herein in terms of various functional components and processing steps. It should be appreciated that such components and steps may be realized by any number of hardware components configured to perform the specified functions.

[0098] The present invention has been described above with reference to various exemplary embodiments and examples, which are not intended to be limiting in describing the full scope of systems and methods of this invention. However, those skilled in the art will recognize that equivalent changes, modifications and variations of the embodiments, materials, systems, and methods may be made within the scope of the present invention, with substantially similar results, and are intended to be included within the scope of the present invention, as set forth in the following claims.

Claims:

1. A method for using a component coupled to a medical device, the method comprising:

interfacing a communication key with a computer cloud;

downloading encrypted authorization codes from the cloud onto key;

severing communication between the cloud and the key;

interfacing the key with a device controller in communication with a medical device;

coupling a component to the medical device;

downloading the authorization codes to at least one of the medical device and the component; and

initiating the component for use when coupled to the medical device.

2. The method according to claim 1, further comprising determining if the component is valid.

3. The method according to claim 1, further comprising:

operating the medical device and the component;

counting a number of treatments performed by the component during the operating the medical device and the component;

providing a limit of the number of treatments performed by the component during the operating the medical device and the component; and

disabling the component upon reaching the limit of the number of treatments performed by the component during the operating the medical device and the component.

4. The method according to claim 1, wherein the authorization codes enables operation of the component.

5. The method according to claim 1, further comprising:

reviewing a current version of software on the controller;

determining if a software update is available on the key; and

downloading the software update to the controller and updating the current version of software with the software update.

6. A treatment system comprising:

a secured key comprising encrypted protected memory;

a secured site located on a computing cloud and configured to securely communicate with the secured key;

an interface configured for secured communication between the secured site and the secured key;

a treatment device;

a device controller in communication with and configured to control the treatment device, the device controller comprising a communication port configured for communication with the secured key; and

a component coupled to the treatment device and in communication with the secured key.

7. The treatment system according to claim 6, further comprising a processor configured to communicate with the secured site and comprising a communication port configured for communication with the secured key.

8. The treatment system according to claim 6, further comprising an authorization code configured to be downloaded from the secured site onto the secured key and further configured to be transmitted from the secured key to the EEPROM, wherein the authorization code is configured to be delivered to the authorization protocol and permit the authorization protocol to enable operation of the component.

9. The treatment system according to claim 6, further comprising:

a treatment counter embedded into the secured key and in communication with the component; and

an expiration function configured to execute after a predetermined number of treatments as clocked by the treatment counter and configured disable operation of the component upon completion of the predetermined number of treatments.

10. The treatment system according to claim 6, further comprising a software update configured to be delivered from the secured site to the secured key and further configured to be uploaded from the secured key to the device controller and configured to update the software rev on running the device controller.

11. The treatment system according to claim 6, further comprising a firewall configured to automatically operate upon operation of the component and configured to prevent any communication to the device controller with the cloud.

12. A method of enabling a treatment device, the method comprising:

downloading an authorization code from a cloud computing network on to a secured electronic key;

interfacing the secured electronic key with component treatment module coupled to a treatment device;

initiating communication between the secured electronic key and the component treatment module;

determining if the component treatment module is enabled to be authorized by the secured electronic key;

downloading the authorization code to the component treatment module;

authorizing the component treatment module with the authorization code; and

enabling operation of the treatment device coupled to the component treatment module, which has been authorized.

13. The method according to claim 12, further comprising the steps of:

disabling the component treatment module, if the component treatment module is not enabled to be authorized by the secured electronic key; and

preventing operation of the treatment device coupled to the component treatment module, which has been disabled.

14. The method according to claim 12, further comprising:

operating the treatment device coupled to the component treatment module, which has been authorized; and

counting on the secured electronic key a number of treatments performed by the component treatment module during the operating the treatment device coupled to the component treatment module, which has been authorized.

15. The method according to claim 14, further comprising:

providing on the secured electronic key a limit of the number of treatments performed by the component treatment module during the operating the treatment device coupled to the component treatment module, which has been authorized; and

disabling the component treatment module upon reaching the limit of the number of treatments performed by the component during the operating the treatment device coupled to the component treatment module, which has been authorized.

16. The method according to claim 12, further comprising establishing a communication interface between the secured electronic key and the cloud computing network before the step of downloading the authorization code from the cloud computing network on to the secured electronic key.

17. The method according to claim 16, further comprising severing the communication interface between the secured electronic key and the cloud computing network after the step of

downloading the authorization code from the cloud computing network on to the secured electronic key.

18. The method according to claim 12, further comprising the steps of:

downloading a software update from the cloud computing network onto the secured electronic key;

notifying the treatment device of the software update upon the step of the initiating communication between the secured electronic key and the component treatment module;

downloading the software update from the secured electronic key to the treatment device; and

intitating the software update on the treatment device.

19. The method according to claim 12, further comprising preventing the secured electronic key from interfacing with the cloud computing network upon the step of the initiating communication between the secured electronic key and the component treatment module.

20. The method according to claim 12, further comprising

collecting information from the treatment device on to the secured electronic key; and

uploading the information from the secured key to the cloud computing network, wherein the information comprises at least one of treatment logs, diagnostic information, and treatment device usage.

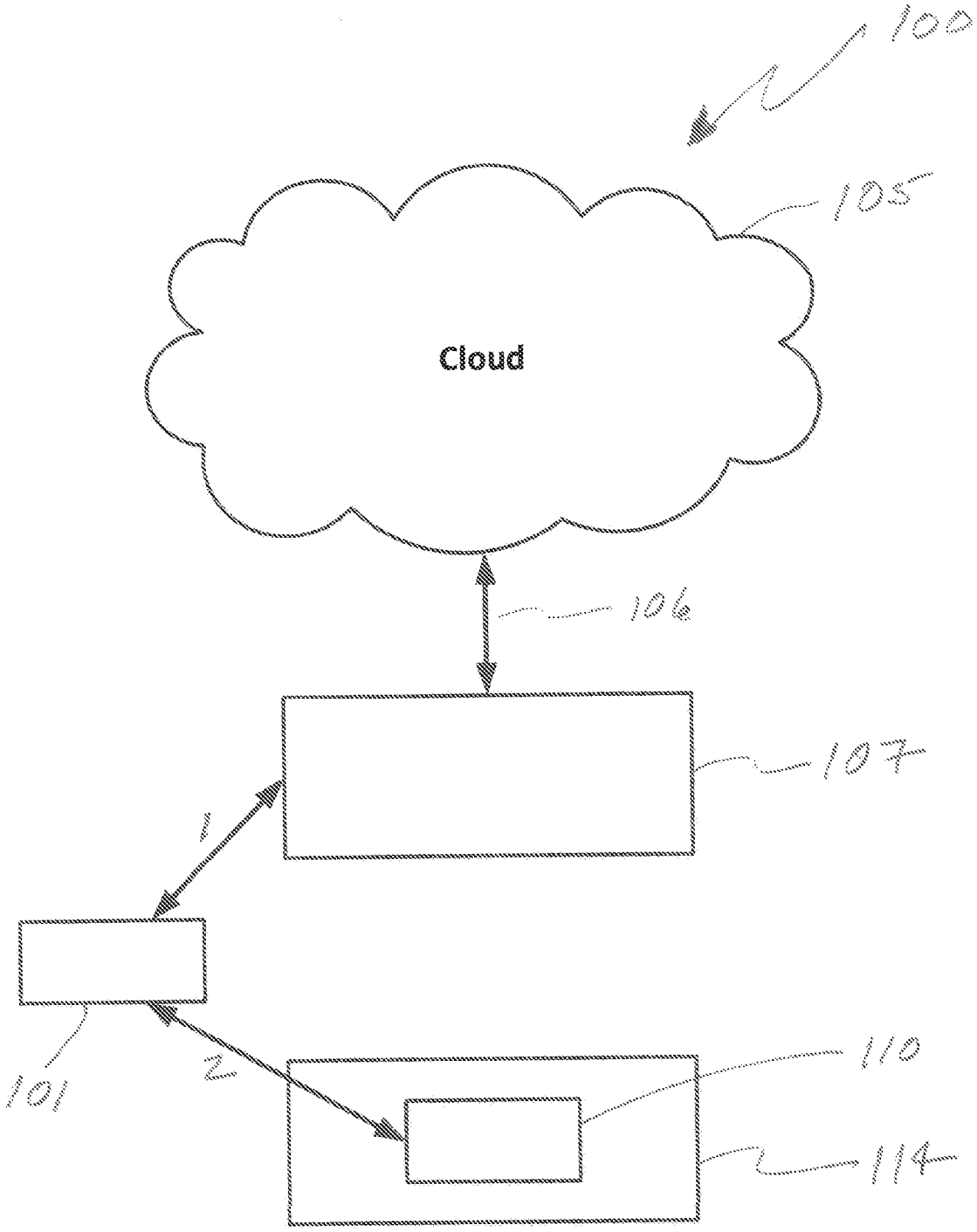

FIG 1

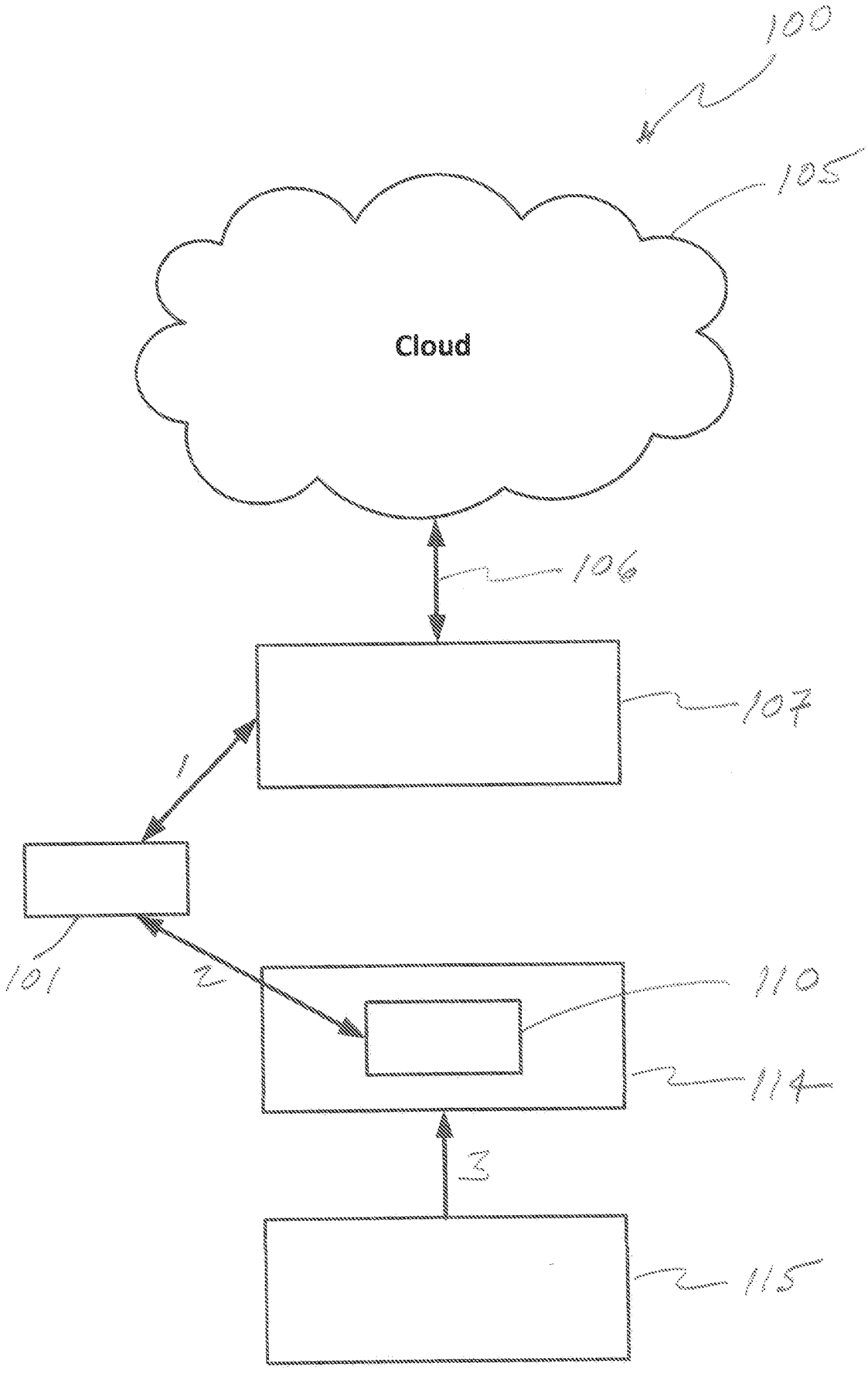

FIG 2

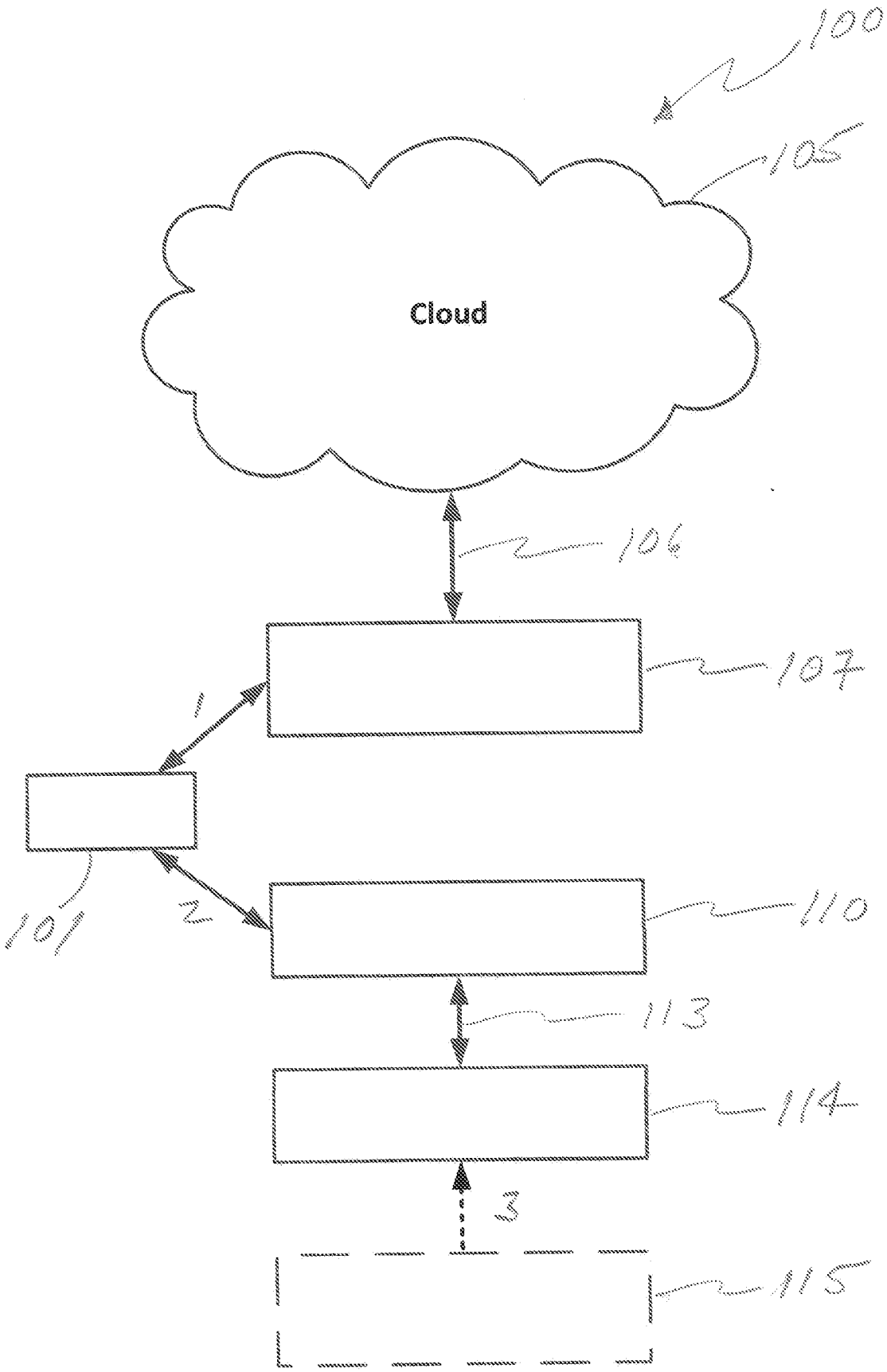

FIG 3

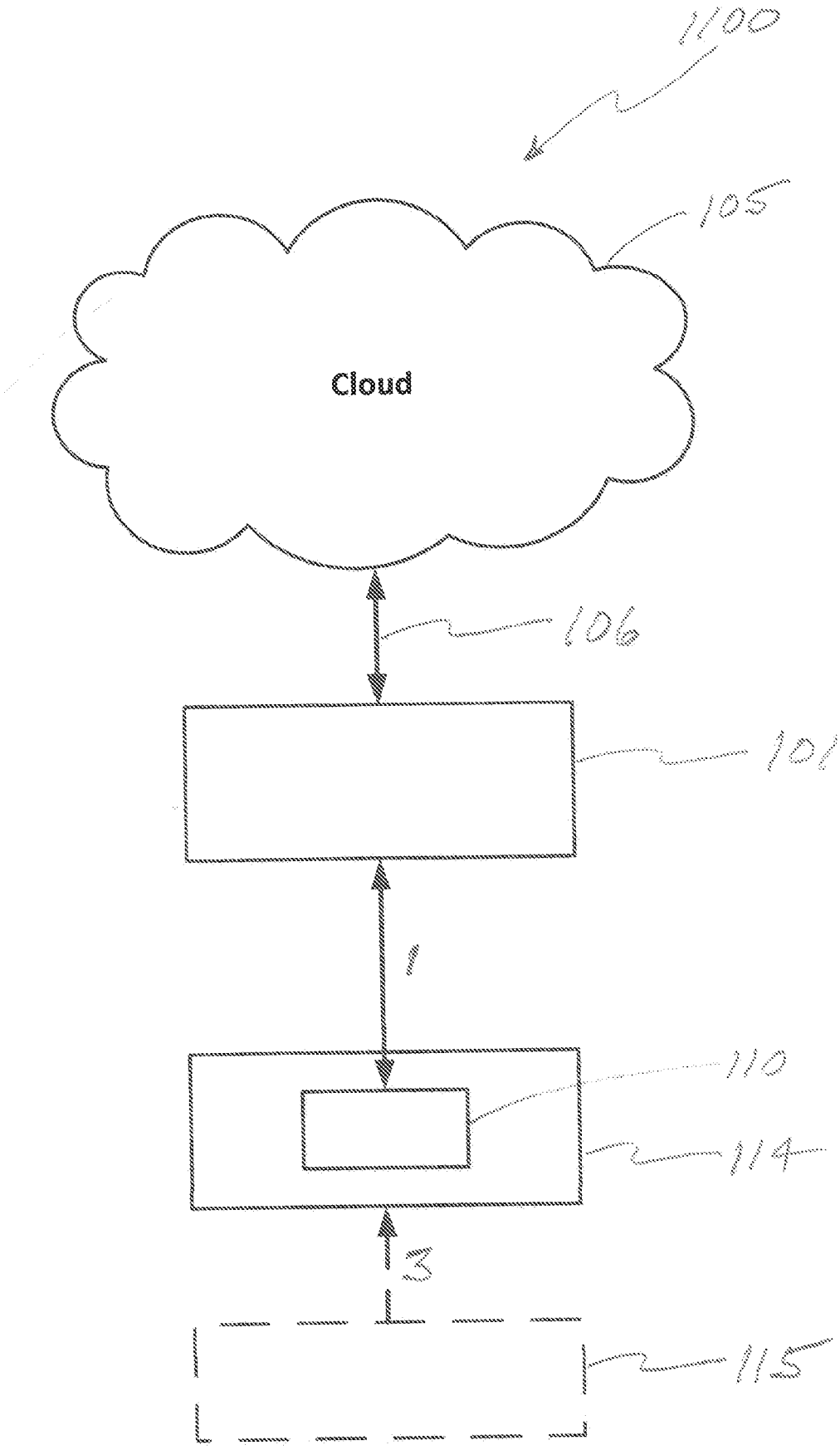

FIG 4

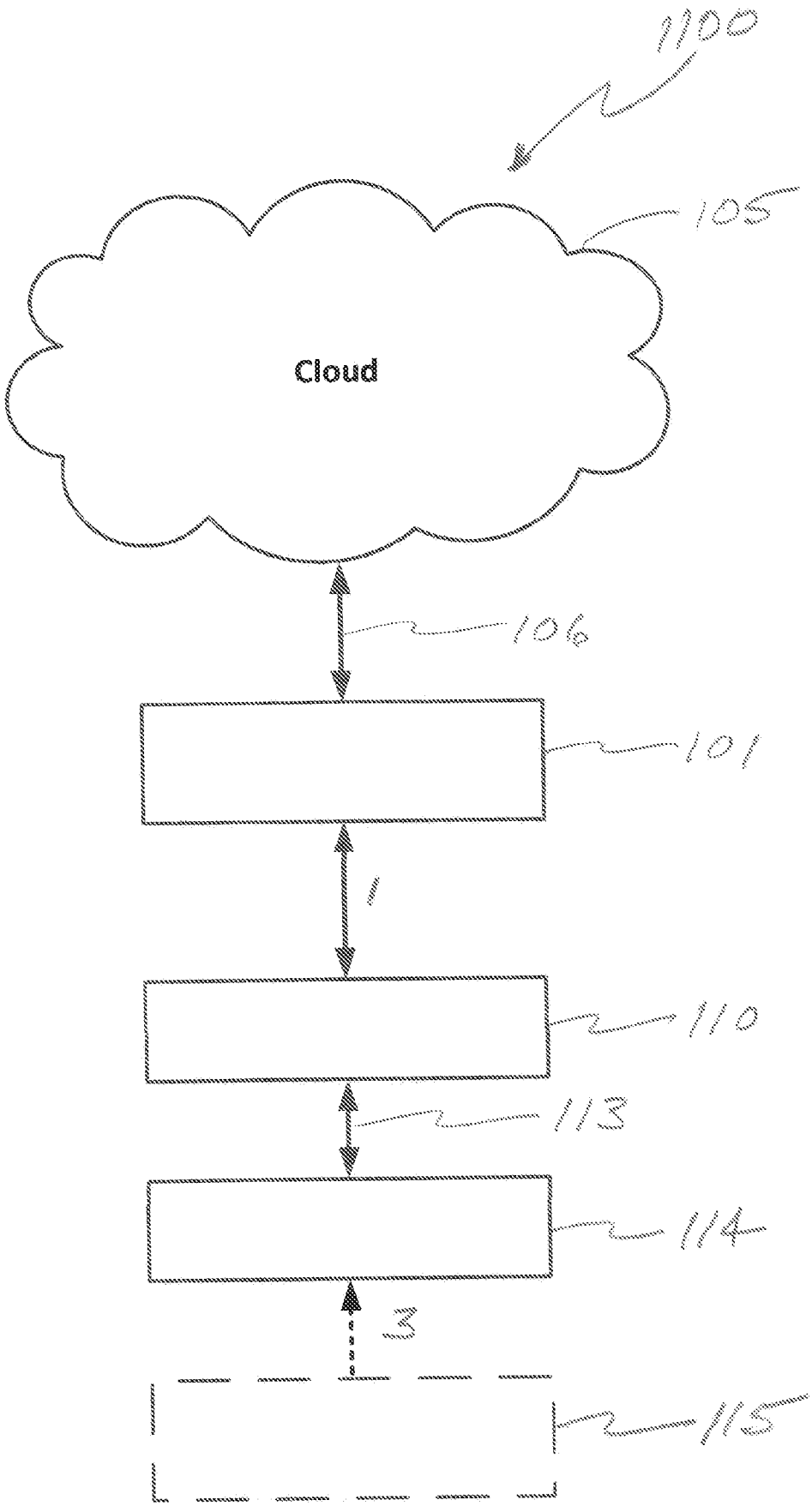

FIG 5

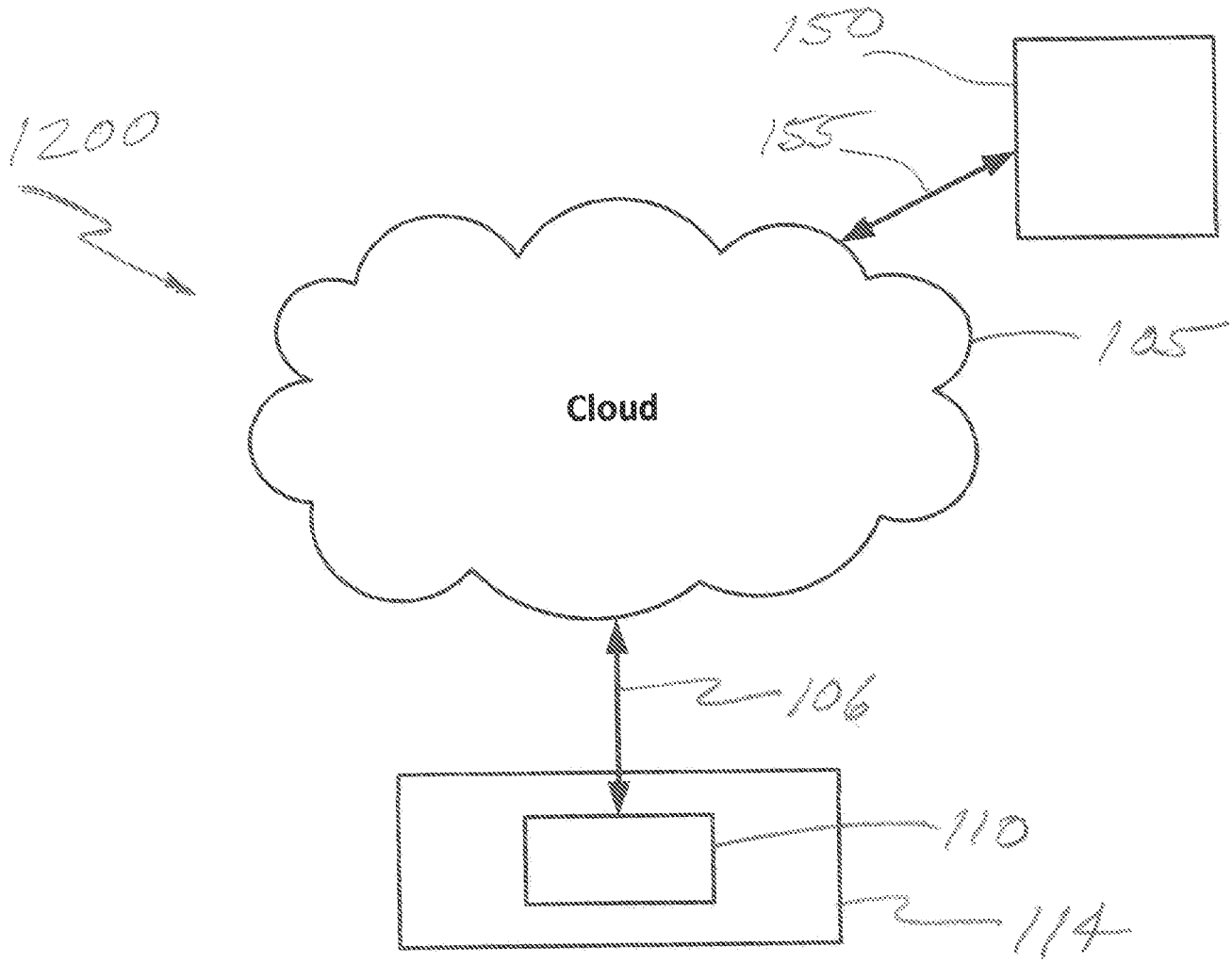

FIG 6

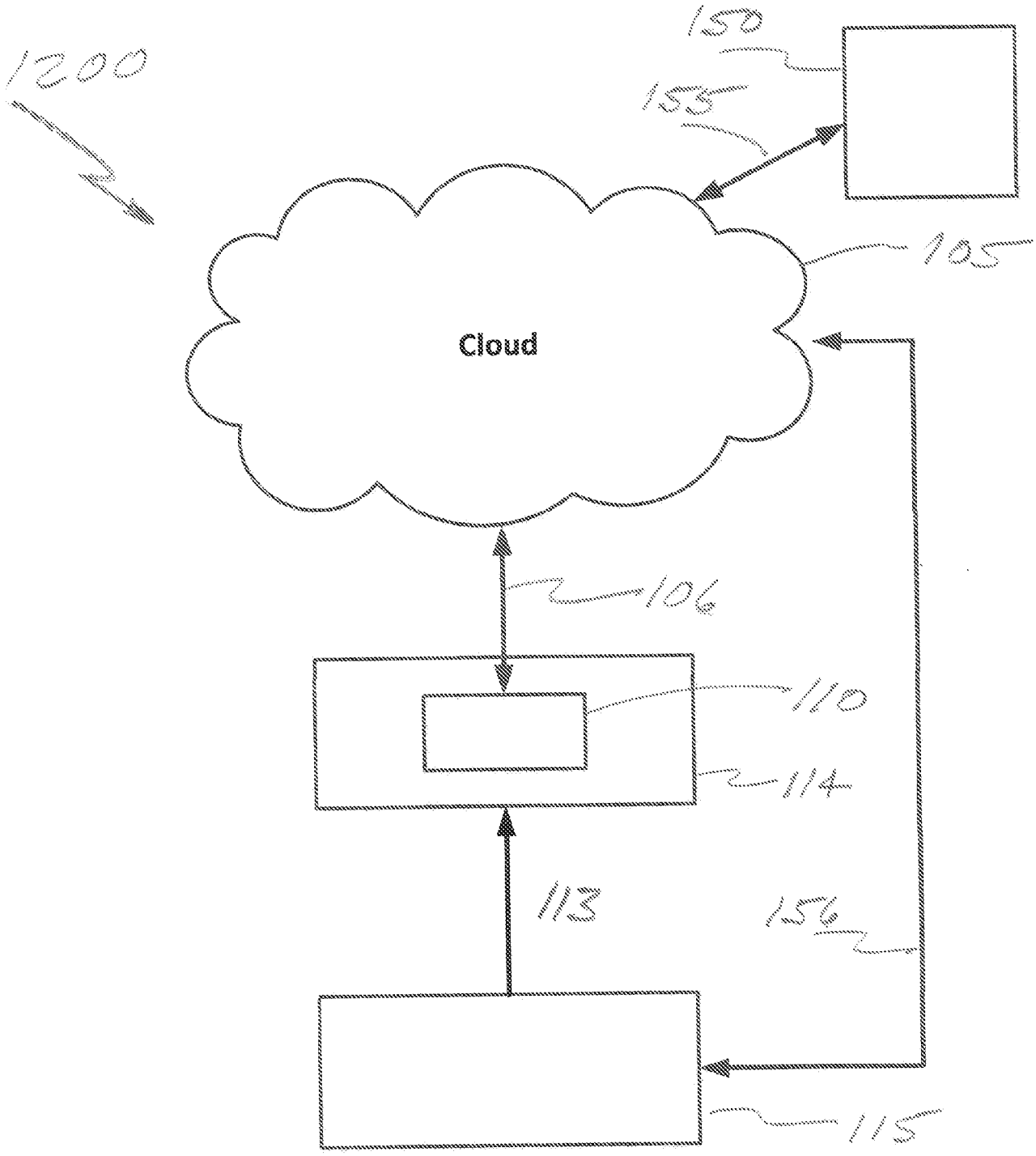

FIG 7

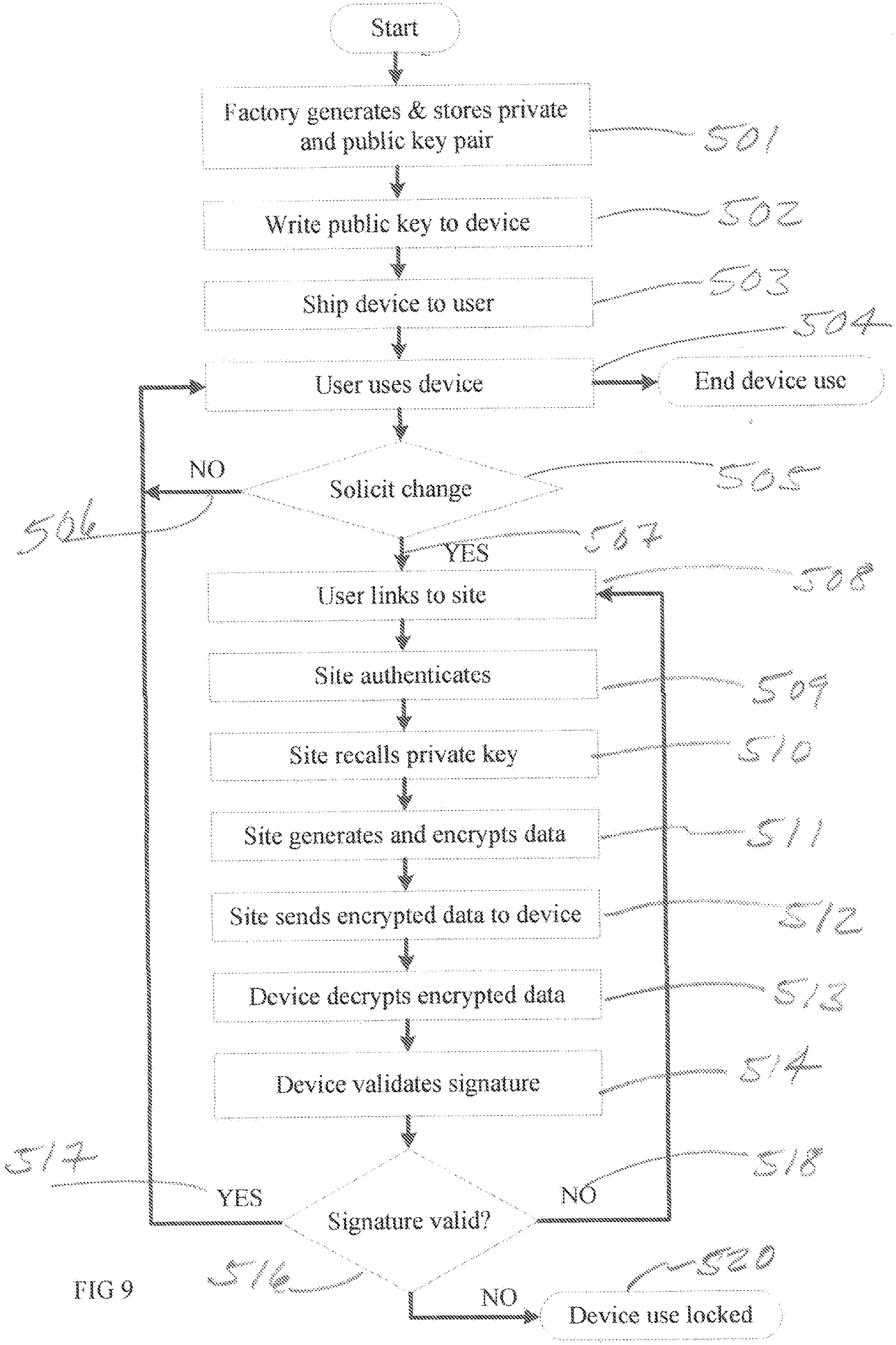
Start
Factory generates & stores private and public key pair
501
Write public key to device
502
Ship device to user
503
User uses device
504
End device use
Solicit change
505
NO
506
YES
507
User links to site
508
Site authenticates
509
Site recalls private key
510
Site generates and encrypts data
511
Site sends encrypted data to device
512
Device decrypts encrypted data
513
Device validates signature
514
Signature valid?
516
517
YES
518
NO
Device use locked
520

FIG 9

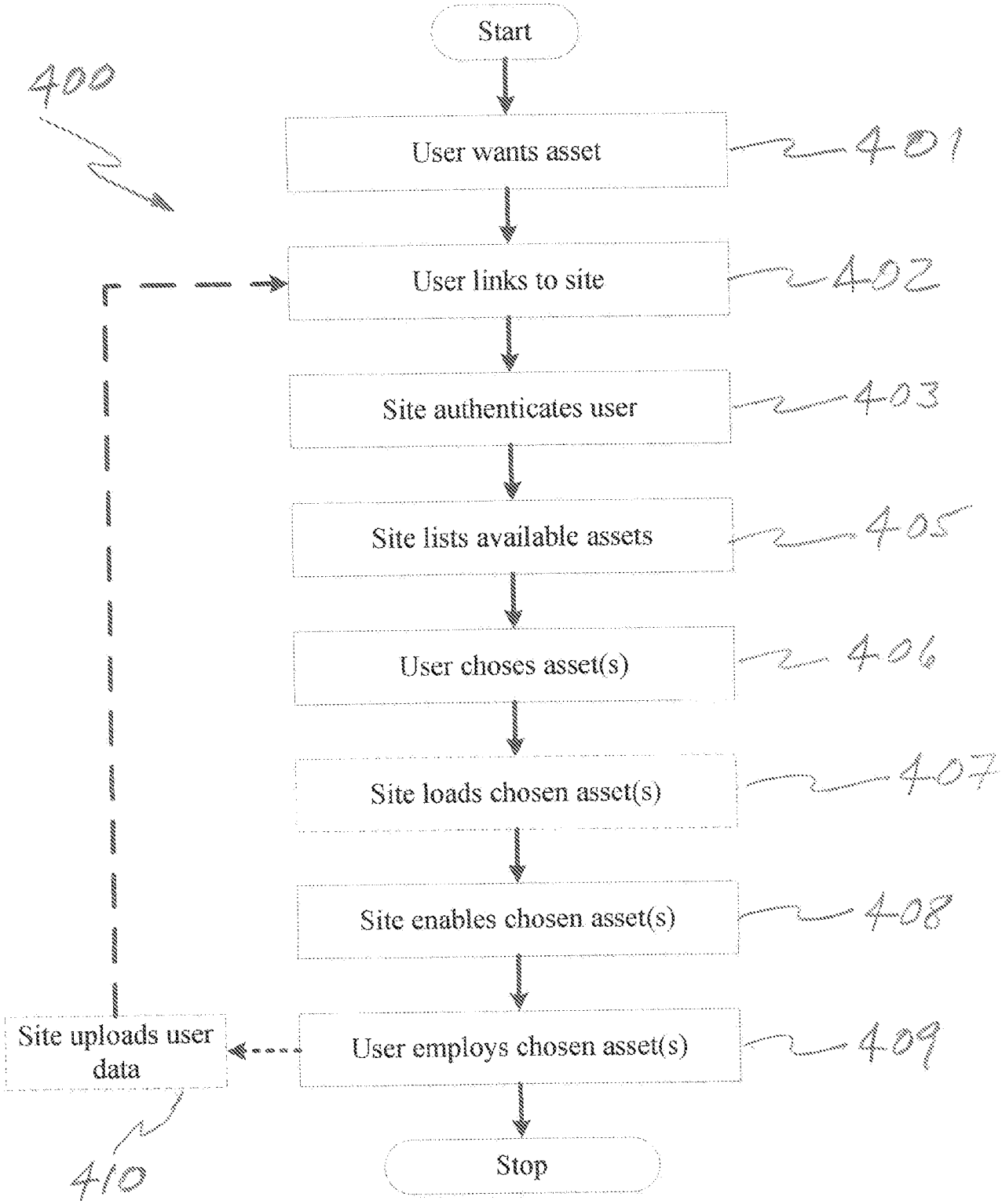
Start
400
User wants asset
401
User links to site
402
Site authenticates user
403
Site lists available assets
405
User choses asset(s)
406
Site loads chosen asset(s)
407
Site enables chosen asset(s)
408
Site uploads user data
User employs chosen asset(s)
409
410
Stop

FIG 8

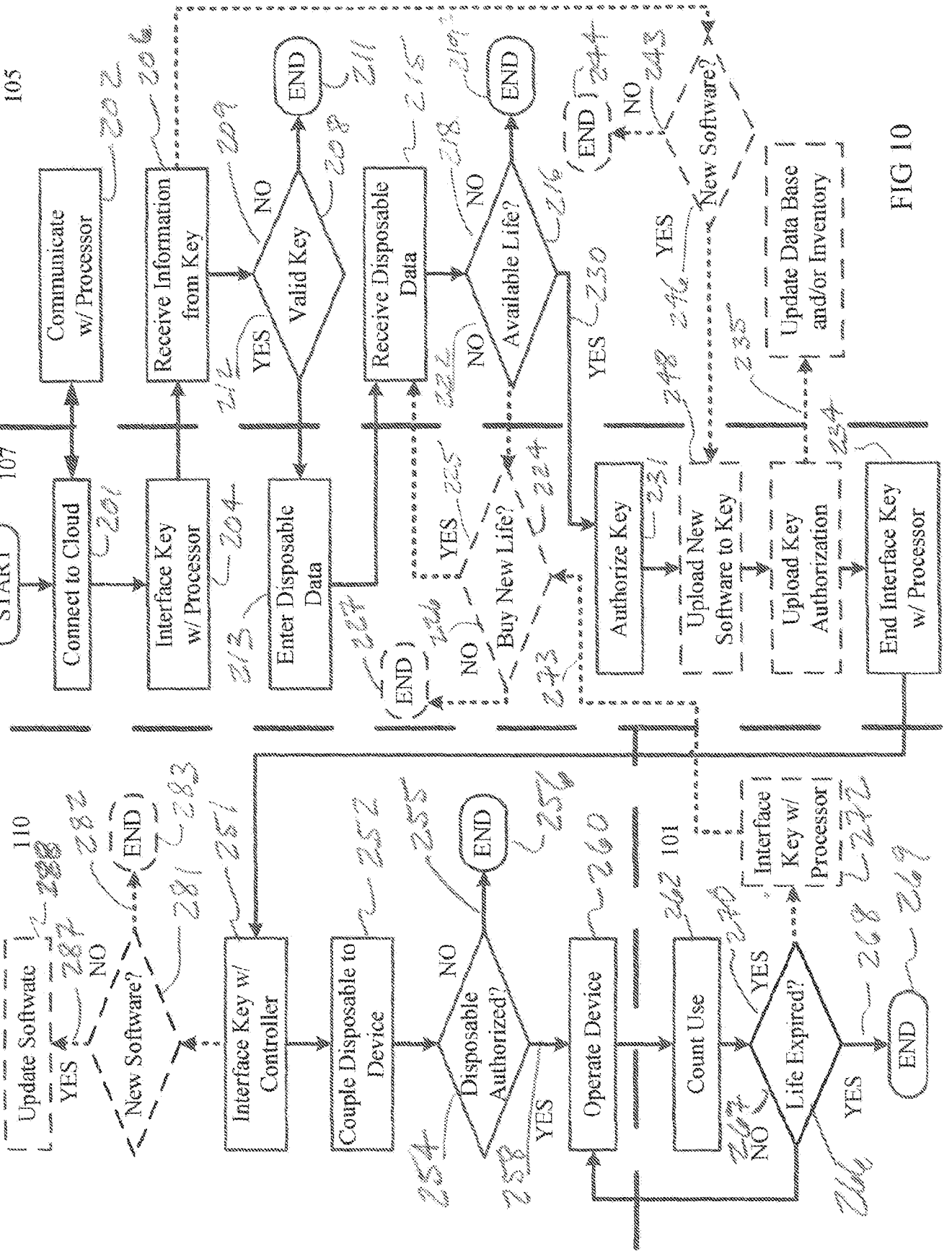
105
107
110
START
Connect to Cloud
201
Communicate w/ Processor
202
Interface Key w/ Processor
204
Receive Information from Key
206
Enter Disposable Data
213
Valid Key
208
NO
209
YES
212
END
211
Receive Disposable Data
214
Available Life?
216
NO
218
YES
224
END
217
Buy New Life?
223
NO
226
YES
225
END
227
Authorize Key
231
YES
230
Upload New Software to Key
248
New Software?
246
YES
NO
243
END
244
Upload Key Authorization
235
Update Data Base and/or Inventory
234
End Interface Key w/ Processor
Update Softwate
288
YES
282
NO
New Software?
281
END
283
Interface Key w/ Controller
251
Couple Disposable to Device
252
Disposable Authorized?
254
NO
255
END
256
YES
258
Operate Device
260
Count Use
262
101
Life Expired?
264
NO
YES
Interface Key w/ Processor
240
268
272
END
269

FIG 10

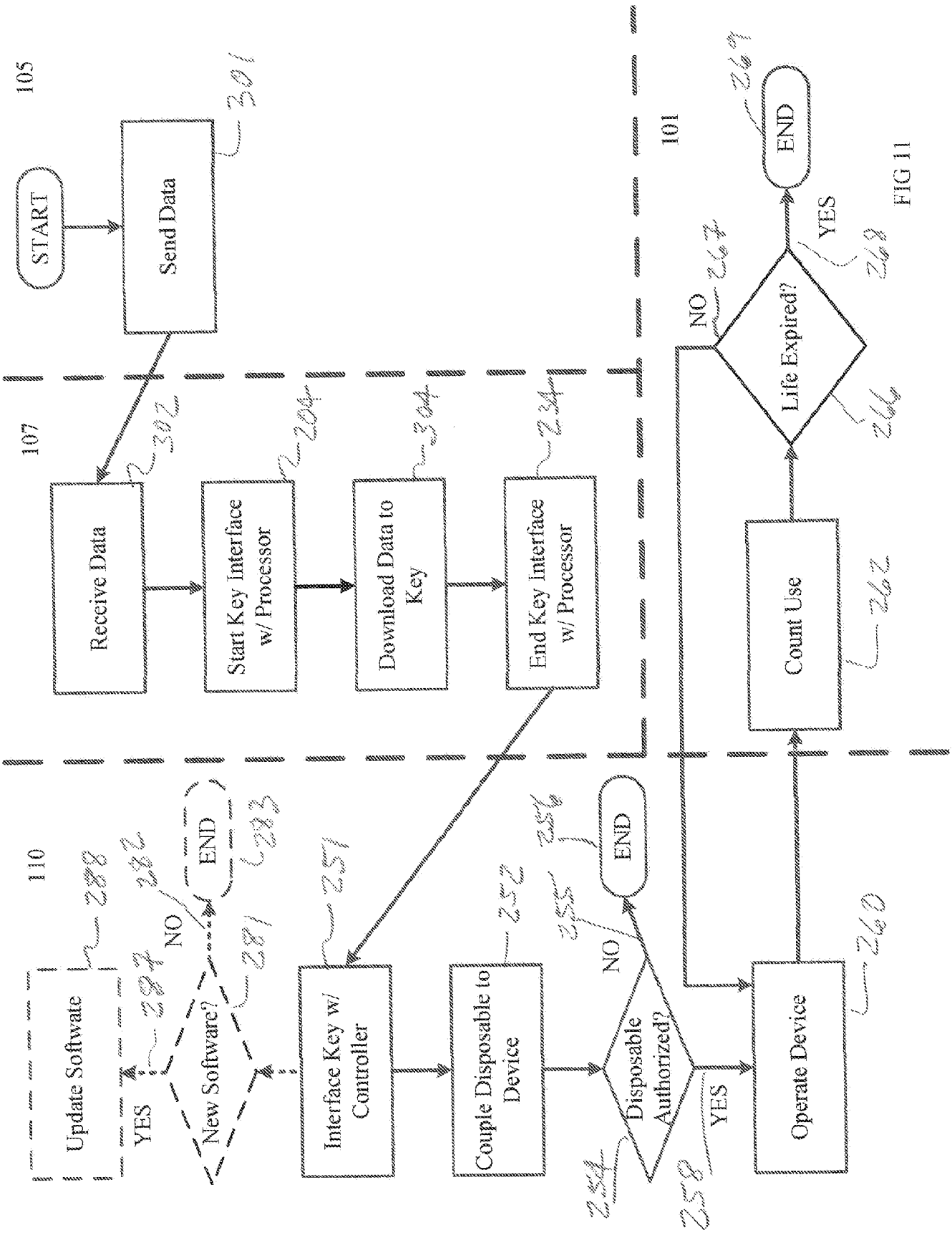
105
107
101
110
START
Send Data
301
Receive Data
302
Start Key Interface w/ Processor
204
Download Data to Key
304
End Key Interface w/ Processor
234
Interface Key w/ Controller
251
Couple Disposable to Device
252
Disposable Authorized?
254
NO
255
END
256
YES
258
Operate Device
260
Count Use
262
Life Expired?
264
NO
266
YES
268
END
269
New Software?
281
NO
282
END
283
YES
284
Update Software
288

FIG 11

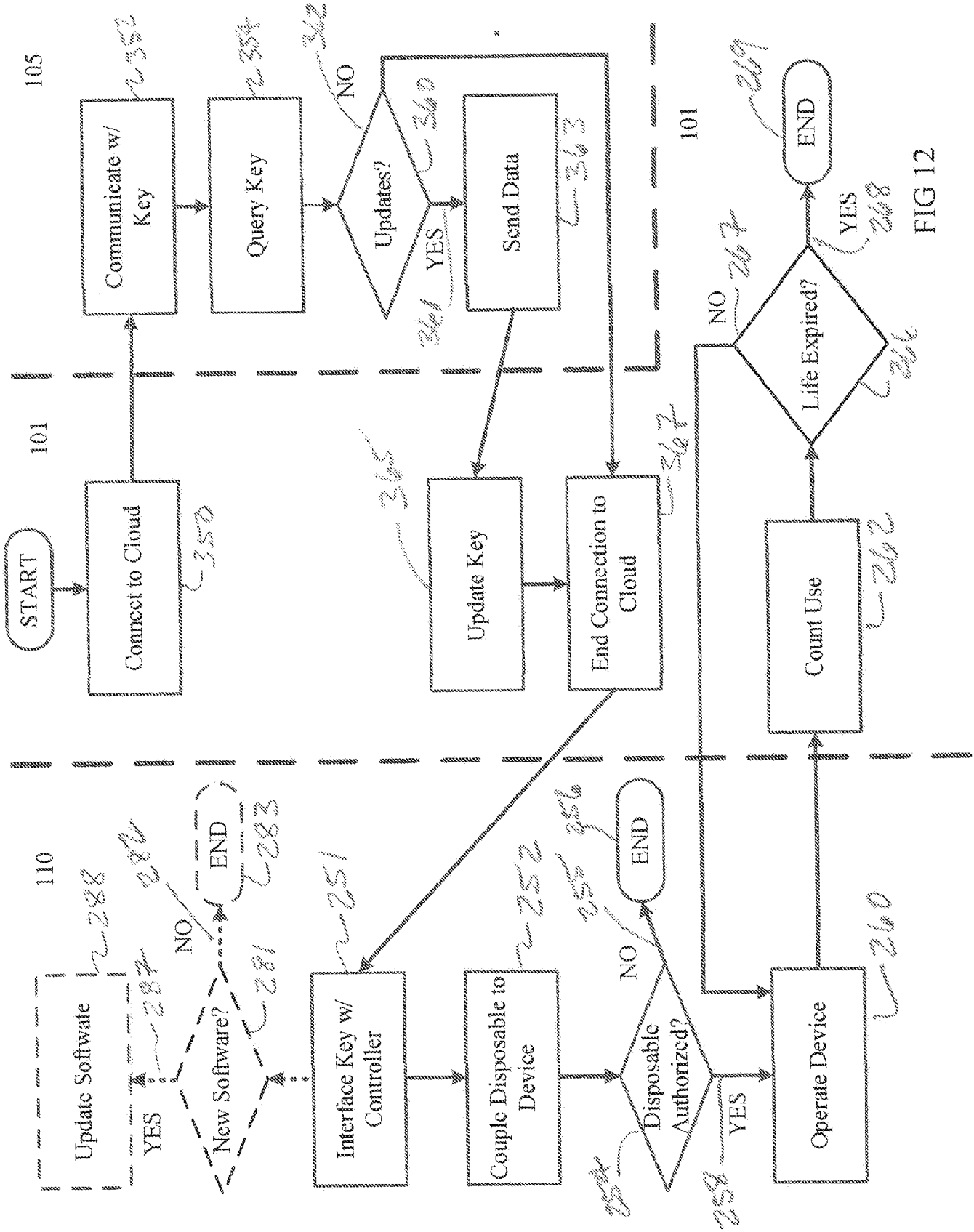
105
101
110
101
START
Connect to Cloud
350
Communicate w/ Key
352
Query Key
354
Updates?
356
NO
YES
358
Send Data
360
Update Key
362
End Connection to Cloud
364
Life Expired?
366
NO
368
YES
369
END
Count Use
262
Operate Device
260
Disposable Authorized?
258
NO
256
YES
254
END
Couple Disposable to Device
252
Interface Key w/ Controller
251
New Software?
281
NO
283
YES
285
Update Software
288
END

FIG 12