(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 2014/143458 A1

(51) International Patent Classification:
H04M 1/60 (2006.01) *H04B 13/00* (2006.01)

(21) International Application Number:
PCT/US2014/015012

(22) International Filing Date:
6 February 2014 (06.02.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/778,944	13 March 2013 (13.03.2013)	US
61/778,975	13 March 2013 (13.03.2013)	US
61/778,913	13 March 2013 (13.03.2013)	US
13/890,319	9 May 2013 (09.05.2013)	US

(71) Applicant: **MOTOROLA MOBILITY LLC** [US/US]; 600 North US Highway 45, Libertyville, Illinois 60048 (US).

(72) Inventors: **CHANDRA, Deepak**; 526 N. Whisman Road, Mountain View, California 94043 (US). **LJUNG, Per Bo Johan**; 5940 Buena Vista Avenue, Oakland, California 94618 (US).

(74) Agents: **BRETSCHER, John T.** et al.; 600 North US Highway 45, Libertyville, Illinois 60048 (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).

[Continued on next page]

(54) Title: COMMUNICATING VIA A BODY-AREA NETWORK

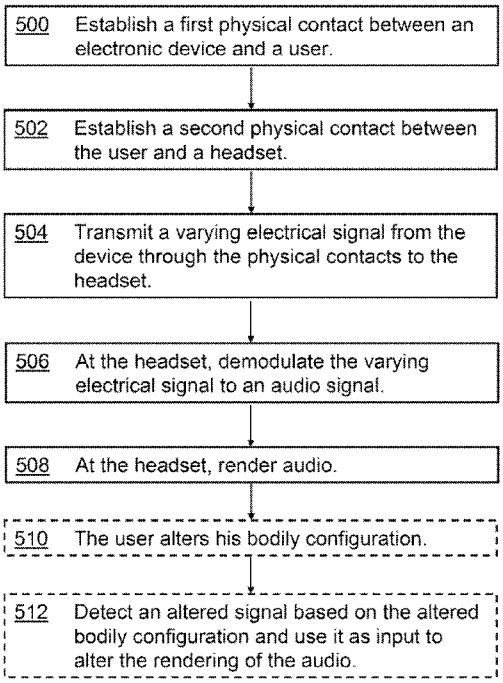


FIG. 5

(57) Abstract: In a first example of "Body-Area Networking", "BAN", a user (100) wishing to access his electronic device (102) ingests a small pill carrying a transmitter (104). The transmitter's signal carries an identification code that traverses the user's BAN and is read (306, 308) by the device (102). If the device (102) recognizes that identification code as authenticate, then the device (102) grants (312) the user (100) the desired access. In another example, the user (100) again swallows a transmitter (104). When the user (100) shakes hands (406) with another person (106), the signal originating at the ingested transmitter (104) is carried across the BAN of the first user (100), travels across the handshake to the BAN of the second user (106), then traverses (408) the second user's BAN to her device (102). In a third example, a media player (102) transmits (504) audio information across the BAN to a headset (110) worn by the user (108). The headset (110) receives (504) the signal, demodulates (506) it, and renders (508) the audio to the user (108).

WO 2014/143458 A1

Published:

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

COMMUNICATING VIA A BODY-AREA NETWORK

TECHNICAL FIELD

[0002] The present disclosure is related generally to electronic communications and, more particularly, to body-area networking.

BACKGROUND

[0003] Recent engineering studies show that electrical signals can be transmitted through a human body. With careful configuration, these signals can be modulated to carry digital information across a so-called "Body-Area Network" ("BAN").

[0004] One company, for example, makes small ingestible pills. Each pill contains the circuitry for a transmitter. When the outer covering of the pill dissolves in a digestive tract, contacts are exposed to stomach acid. The stomach acid acts as a dielectric to power the transmitter. (For safety's sake, the pill contains no other power source.) When powered up, the transmitter repeatedly sends out a weak electrical signal. The signal is carried across the BAN to a receiving device located outside, but in physical contact with, the ingestor's body. The receiver demodulates the signal into an identification code. The transmitter continues to send out its signal until the process of digestion dissolves the pill. The transmitter typically transmits for a total of five to seven minutes.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0005] While the appended claims set forth the features of the present techniques with particularity, these techniques, together with their objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

[0006] Figures 1a, 1b, and 1c are overviews of representative environments in which the present techniques may be practiced;

[0007] Figure 2 is a generalized schematic of some of the devices of Figure 1;

[0008] Figures 3A and 3B together form a flowchart of a representative method for allowing access to a device based on a signal received from an ingested transmitter;

[0009] Figures 4A and 4B together form a flowchart of a representative method for delivering information about one person to another person; and

[0010] Figure 5 is a flowchart of a representative method for transmitting audio information via a BAN.

DETAILED DESCRIPTION

[0011] Turning to the drawings, wherein like reference numerals refer to like elements, techniques of the present disclosure are illustrated as being implemented in a suitable environment. The following description is based on embodiments of the claims and should not be taken as limiting the claims with regard to alternative embodiments that are not explicitly described herein.

[0012] The emerging technology of BAN communications can be profitably used in a variety of situations. Consider first the communications environment of Figure 1a. Here, a user 100 wishes to access his electronic device 102. For security's sake, the device 102 will not allow the user 100 to access it until he provides some identification information. Traditionally, the user 100 could enter a user name and a password, or the device 102 could recognize a signature or fingerprint submitted by the user 100. Aspects of the present invention, however, eliminate the need for these techniques. The user 100 ingests a small pill carrying a transmitter 104. The transmitter's signal carries an identification code that traverses the user's BAN and is read by the device 102. If the device 102 recognizes that identification code as authenticate (using techniques described below), then the device 102 grants the user 100 the desired access.

[0013] Another use of BAN communications is illustrated in Figure 1b. Again, the user 100 has swallowed a transmitter 104 that constantly transmits an identification code. When the user 100 shakes hands with another person 106, it is a device 102 (not shown) on this other user 106 that receives the signal. That is to say,

the signal originating at the ingested transmitter 104 is carried across the BAN of first user 100, travels across the handshake to the BAN of the second user 106, then traverses the second user's BAN to her device 102. In one application of this two-BAN scenario, the second user's device 102 runs a virtual "Farley File" application: When it receives the identification code sent by the transmitter 104, it recognizes the code and associates it with a particular person, here the first user 100. That recognition can make use of a contacts file on the device 102 or an online database, for example. The Farley File application then presents this information to the second user 106 to refresh her memory of whom it is she is currently meeting. Other applications of this two-BAN scenario are discussed below in relation to Figure 4.

[0014] In the examples of Figures 1a and 1b, the electronic device 102 receives a signal coming through the BAN. The example of Figure 1c shows that the device 102 can also transmit across the BAN. The user 108 is wearing a headset 110. Rather than wiring the headset to a media-player device 102 (not shown) or connecting via a short-range radio protocol such as Bluetooth, the media player 102 transmits audio information across the BAN to the headset 110. The headset 110 receives the signal, demodulates it, and renders the audio to the user 108. The particular headset 110 of Figure 1c also includes a microphone, and the headset 110 can transmit voice captured by the microphone across the BAN to the media-player device 102. If, of course, the media player 102 also includes a wide-area communications capability (e.g., it is a cellular telephone), then it can transfer sounds and other information between the headset 110 and remote locations to support, for example, a telephone call, a media download, or web-site access.

[0015] Figure 2 shows the major components of a representative electronics device 102, 110. These devices 102, 110 could be, for example, a smartphone, tablet, personal computer, electronic book, or gaming controller. In some situations, the device 102, 110 could be in the form of a watch, a pair of eyeglasses, a headset, a set-top box, an automated teller machine, a cash register, an order-entry device, a lock, a handle, or a media player.

[0016] The CPU 200 of the electronics device 102, 110 includes one or more processors (i.e., any of microprocessors, controllers, and the like) or a processor and memory system which processes computer-executable instructions to control the operation of the device 102, 110. In particular, the CPU 200 supports aspects of the present disclosure as illustrated in Figures 3 through 5, discussed below. The device 102, 110 can be implemented with a combination of software, hardware, firmware, and fixed-logic circuitry implemented in connection with processing and control circuits, generally identified at 202. Although not shown, the device 102, 110 can include a system bus or data-transfer system that couples the various components within the device 102, 110. A system bus can include any combination of different bus structures, such as a memory bus or memory controller, a peripheral bus, a universal serial bus, and a processor or local bus that utilizes any of a variety of bus architectures.

[0017] The electronics device 102, 110 also includes one or more memory devices 204 that enable data storage, examples of which include random-access memory, non-volatile memory (e.g., read-only memory, flash memory, EPROM, and EEPROM), and a disk storage device. A disk storage device may be implemented as any type of magnetic or optical storage device, such as a hard disk drive, a recordable or rewriteable disc, any type of a digital versatile disc, and the like. The device 102, 110 may also include a mass-storage media device.

[0018] The memory system 204 provides data-storage mechanisms to store device data 212, other types of information and data, and various device applications 210. An operating system 206 can be maintained as software instructions within the memory 204 and executed by the CPU 200. The device applications 210 may also include a device manager, such as any form of a control application or software application. The utilities 208 may include a signal-processing and control module, code that is native to a particular component of the electronics device 102, 110, a hardware-abstraction layer for a particular component, and so on.

[0019] The electronics device 102, 110 can also include an audio-processing system 214 that processes audio data and controls an audio system 216 (which may

include, for example, speakers). A visual-processing system 218 processes graphics commands and visual data and controls a display system 220 that can include, for example, a display screen. The audio system 216 and the display system 220 may include any devices that process, display, or otherwise render audio, video, display, or image data. Display data and audio signals can be communicated to an audio component or to a display component via a radio-frequency link, S-video link, High-Definition Multimedia Interface, composite-video link, component-video link, Digital Video Interface, analog audio connection, or other similar communication link, represented by the media-data ports 222. In some implementations, the audio system 216 and the display system 220 are components external to the device 102, 110. Alternatively (e.g., in a cellular telephone), these systems 216, 220 are integrated components of the device 102, 110.

[0020] The electronics device 102, 110 can include a communications interface which includes communication transceivers 224 that enable wired or wireless communication. Example transceivers 224 include Wireless Personal Area Network radios compliant with various IEEE 802.15 standards, Wireless Local Area Network radios compliant with any of the various IEEE 802.11 standards, Wireless Wide Area Network cellular radios, Wireless Metropolitan Area Network radios compliant with various IEEE 802.16 standards, and wired Local Area Network Ethernet transceivers.

[0021] The electronics device 102, 110 may also include one or more data-input ports 226 via which any type of data, media content, or inputs can be received, such as user-selectable inputs (e.g., from a keyboard, from a touch-sensitive input screen, or from another user-input device), messages, music, television content, recorded video content, and any other type of audio, video, or image data received from any content or data source. The data-input ports 226 may include USB ports, coaxial-cable ports, and other serial or parallel connectors (including internal connectors) for flash memory, storage disks, and the like. These data-input ports 226 may be used to couple the device 102, 110 to components, peripherals, or accessories such as microphones and cameras.

[0022] Finally, the electronics device 102, 110 may include any number of "other sensors" 228. These sensors 228 can include, for example, accelerometers, a GPS receiver, compass, magnetic-field sensor, and the like.

[0023] Figures 3a and 3b together present a representative method for using BAN communications in the environment of Figure 1a.

[0024] Steps 300 and 302 prepare the ground for the later authentication step 312. Each ingestible transmitter 104 can be given a different identification code. In a very simple example of step 300, a "white list" of the identification codes of the transmitters 104 that will be used by this user 100 are entered into his device 102. This process is ideally a secure one because the security of later authentication is based on it. If the ingestible transmitters 104 are prescription items, then their identification codes can be encoded onto their packaging and those codes read by the device 102. Alternatively, the codes could be downloaded from the pharmacy's server to the device 102 when the user 100 picks up the prescribed transmitters 104. More secure, the packaging (or pharmacy download) could include a unique identifier that the device 102 uses when accessing a secure web server to download the identification codes.

[0025] As another known security technique, the identification codes associated with the transmitters 104 can be placed in a set sequence. If a nefarious agent manages to get hold of a transmitter 104 but uses it out-of-sequence, then he would be denied access in step 312, described below.

[0026] A one-time-pad security mechanism can also be used along with the identification codes of the individual transmitters 104. Though highly secure, one-time pads are often an administrative nuisance and are thus mostly useful where access to the device 102 needs to be highly controlled (e.g., rather than being a personal cellular telephone, the device 102 is an electronic lock mediating entrance into a secured facility).

[0027] Also in step 300, the user 100 can be identified to the device 102, for example by storing a profile of the user 100 on the device 102.

[0028] Where more than one user 100 should be allowed access to the device 102 (e.g., all members of one family may use the same device 102), then the identification codes can be associated with all of the relevant users 100, and all of the relevant users 100 can be associated with the device 102.

[0029] Other known security techniques can be implemented as appropriate, given the level of security desired.

[0030] With the security preliminaries established, if necessary, the user 100 begins the actual identification method of Figure 3 by establishing a physical contact with the device 102 in step 304. Tests have shown that when the device 102 is a smartphone, a two-finger contact, using one finger from each hand, tends to be more reliable than using two fingers on the same hand. The device 102 may expose two dedicated contact points. Alternatively, one contact point may be the capacitive touch-screen of the device 102, while the other contact point is a frame of the device 102. For devices 102 with form factors other than the typical smartphone, other contact placements may be appropriate.

[0031] In step 306, a varying electrical signal originating at the ingested transmitter 104 traverses the BAN of the user 100 until it is detected, via the physical contact established in step 304, by the device 102. Different transmitters 104 may be developed that use different signaling mechanisms. Thus, the detected current could be, for example, a direct electrical current, an alternating current, or a varying capacitive field.

[0032] In any case, the device 102 demodulates the received signal to an identification code in step 308. The received signal can also include information beyond this identification code. This possibility is discussed below in relation to optional step 310.

[0033] In step 312, the identification code is checked and, if appropriate, the user 100 is allowed further access to the device 102. The checking here can call in all of the authentication mechanisms discussed above in relation to steps 300 and 302. If, for example, a specific sequence of codes has been defined, then one particular

identification code be legitimate, but if it is encountered out-of-sequence, then it would be rejected.

[0034] The allowed "further access" can have any number of meanings. Even if security is not an issue, the device 102 can configure itself according to the stated profile and preferences of this particular user 100, that is, it can give the user 100 his preferred login environment. Just as with traditional password-protected systems, different users 100 can be allowed different levels of access, with some users being allowed to alter parameters of the device 102. Also, the access can vary dramatically with the form factor of the device 102. If the device 102 is an electronic lock, then it could allow the user 100 to open a door. If the device 102 is an automated teller machine, it may automatically bring up a screen displaying the user's current checking balance. In general, the techniques of Figure 3 can be implemented with just about any device 102 that recognizes its users 100.

[0035] Returning to optional step 310, the transmitter 104 can send information beyond its identification code. If the ingestible pill that carries the transmitter 104 also carries a sensor (e.g., a temperature or stomach-acid sensor), then readings from that sensor could be sent to the device 102. If, for example, a device 102 carried by a fireman detects, from body-temperature information transmitted by an ingestible sensor, that the fireman's core temperature is dangerously elevated, then the device 102 could warn the fireman to withdraw or could call for assistance.

[0036] In optional step 314 of Figure 3b, the device 102 can note the timing and frequency with which the user 100 ingests the transmitters 104. For transmitters 104 associated with prescribed medication, if the device 102 has access to the desired medication schedule, then it can remind the user 100 if he seems to have missed taking his medicine on time. By looking at the user's calendar, the device 102 might note that the user will be traveling soon and will remind the user 100 to pack enough transmitters 104 for the duration of the trip.

[0037] As an extension of the method already described, the device 102 can transmit back over the BAN of the user 100 to another device (step 316). An example of this option is more fully described in the text accompanying Figures 1c and 5.

[0038] Step 318 gives a few scenarios where the device 102 may optionally cease to trust the identification code read in step 308. As an added security option, if the user 100 uses a non-pill based authentication mechanism (e.g., a fingerprint scanner), then the device 102 will ignore the identification code. If another identification code is received (e.g., if the user 100 ingests another transmitter 104), then the first identification code would no longer be trusted. This scenario could also occur when a sophisticated transmitter 104 changes the code that it is transmitting: Again, the earlier code is no longer to be trusted. As a final option, a time window can be set wherein the identification code is accepted. If the code is still being received after the window closes, then something strange may be going on, and the code is no longer trusted. (Current transmitters 104 only work for five to seven minutes before stomach acid dissolves them into inoperability. Thus, any code received for longer than seven minutes may be fraudulent. While future transmitters 104 may last longer, it is anticipated that they may also have a relatively fixed time window of acceptability.)

[0039] The representative method of Figures 4a and 4b can be used in the BAN-communications scenario of Figure 1b. Some of the steps of this method are similar to those of the method of Figures 3a and 3b. As in that previous method, preliminary authentication mechanisms may be implemented (steps 400 and 402 of Figure 4a.)

[0040] In step 404, the user 106 of Figure 1b establishes a physical contact with her electronic device 102. (See step 304 of Figure 3a.)

[0041] The user 106 establishes a physical contact (e.g., she shakes hands) with another user 100 in step 406. It is this user 100 who has ingested a transmitter 104. The signal emitted by that transmitter 104 traverses the BAN of the user 100, crosses over via the handshake, traverses the BAN of the user 106, and is read by her device 102 in step 408.

[0042] The reading of the signal (step 408) and the demodulating of the signal (step 410 and optional step 412) can be as performed above in steps 306 through 310 of Figure 3a.

[0043] Then in step 414 of Figure 4b, the device 102 uses the identification code to retrieve some information about the user 100. For example, the identification code is associated (in step 400 of Figure 4a) with a person in the device's contact list. The device 102 retrieves that contact information (or possibly updates the contact information by pulling information from the web) and passes it along to the user 106 in step 416. If the user 106 is wearing an earbud, for example, the device 106 can "whisper" the name of the person 100 in her ear. Other information, if available, can be provided such as the last time she met this person 100, the name of the organization he represents, and the like. Thus, the user 106 may be spared the embarrassment of having to admit that she does not recognize the user 100.

[0044] The BAN-communications scenario of Figure 1c differs from the previous two because it does not involve an ingestible transmitter 104. However, many of the techniques discussed above apply here as well.

[0045] In steps 500 and 502, the user 108 establishes a first physical contact between herself and her electronic device 102 and establishes a second physical contact between herself and a headset 110 (which could involve simply placing earbuds in her ears).

[0046] Her device 102 acts as a media-playback device by sending, in step 504, audio information (which could be stereo) across the first physical contact, through the BAN of the user 108, and across the second physical contact to the headset 110.

[0047] The headset 110 receives the signal in step 506, demodulates it into an audio signal, and plays the audio to the user 108 (step 508). Optionally, a signal can be sent in the other direction from a microphone on the headset 110 to the device 102.

[0048] Of special interest are optional steps 510 and 512. When the user 108 alters her bodily configuration (step 510), she changes the transmission characteristics of her BAN. If the change is great enough, it can be detected either by the media player 102 or by the headset 110. The detected change can be interpreted as a playback command (step 512). Thus, for example, if the user 108 draws her right hand down her left forearm, that might mean that she wishes to turn down the volume.

Other gestures could be devised that would be interpreted as other well known playback commands, such as pause, fast-forward, change stations, and the like.

[0049] In view of the many possible embodiments to which the principles of the present discussion may be applied, it should be recognized that the embodiments described herein with respect to the drawing figures are meant to be illustrative only and should not be taken as limiting the scope of the claims. Therefore, the techniques as described herein contemplate all such embodiments as may come within the scope of the following claims and equivalents thereof.

CLAIMS

We claim:

1. A method of transmitting audio information from an electronic device (102) to a headset (110), the method comprising:

concurrently establishing (500) a first physical contact between the electronic device (102) and a user (108) and establishing (502) a second physical contact between the headset (110) and the user (108);

transmitting (504), by the electronic device (102) via the first and second physical contacts to the headset (110), a first varying electrical signal;

demodulating (506), by the headset (110), the first varying electrical signal to an audio signal; and

based, at least in part, on the audio signal, rendering (508), by the headset (110), audio.

2. The method of claim 1 wherein the first varying electrical signal comprises an element selected from the group consisting of: a direct electrical current, an alternating electrical current, and a varying capacitive field.

3. The method of claim 1 wherein the audio signal comprises a plurality of audio channels.

4. The method of claim 1 further comprising:

altering, by the user, a configuration of a body of the user;

detecting, by a device selected from the group consisting of: the headset and the electronic device, an alteration in a second electrical signal, the signal alteration associated with the alteration of the configuration of the user's body; and

based, at least in part, on the detected signal alteration, altering the rendering of the audio.

5. The method of claim 4 wherein the second electrical signal is the first varying electrical signal.

6. The method of claim 4 wherein altering the rendering of the audio comprises performing an element selected from the group consisting of: altering a playback volume, pausing, stopping, rewinding, fast-forwarding, swapping audio channels from left to right, selecting a next track of an audio program, and switching to another audio program.

7. An electronic device (102) configured for transmitting audio information to a headset (110), the electronic device (102) comprising:

a communications interface (224) comprising two electrodes and configured for establishing (500) a first physical contact with a user (108); and

a processor (200) operatively connected to the communications interface (224) and configured for:

transmitting (504), to the headset (110) via the first physical contact and via a second physical contact between the headset (110) and the user (108), a first varying electrical signal.

8. A method of receiving transmitted audio information, the method comprising:

establishing (502) a physical contact between a headset (110) and a user (108);

receiving (504), by the headset (110) via the physical contact, a first varying electrical signal;

demodulating (506), by the headset (110), the first varying electrical signal to an audio signal; and

based, at least in part, on the audio signal, rendering (508), by the headset (110), audio.

9. The method of claim 8 further comprising:

altering, by the user, a configuration of a body of the user;

detecting, by the headset, an alteration in a second electrical signal, the signal alteration associated with the alteration of the configuration of the user's body; and

based, at least in part, on the detected signal alteration, altering the rendering of the audio.

10. A headset (110) configured for receiving transmitted audio information, the headset (110) comprising:

a communications interface (224) comprising two electrodes and configured for establishing a physical contact with a user (108); and

a processor (200) operatively connected to the communications interface (224) and configured for:

receiving (504), via the physical contact, a first varying electrical signal;

demodulating (506), by the headset (110), the first varying electrical signal to an audio signal; and

based, at least in part, on the audio signal, rendering (508) audio.

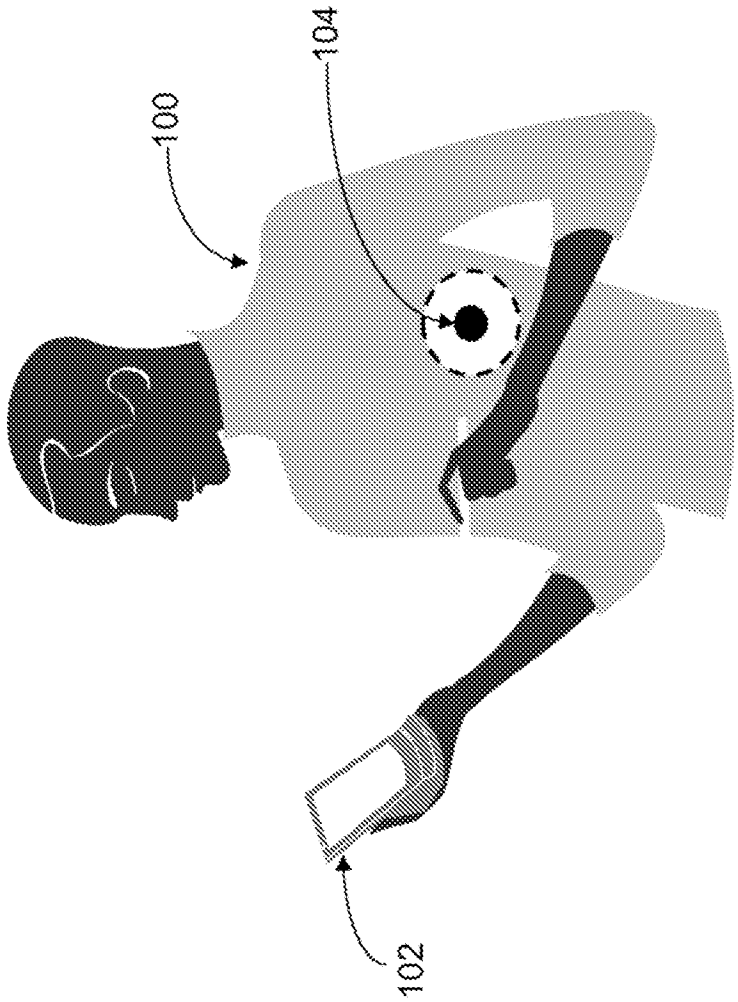


FIG. 1A

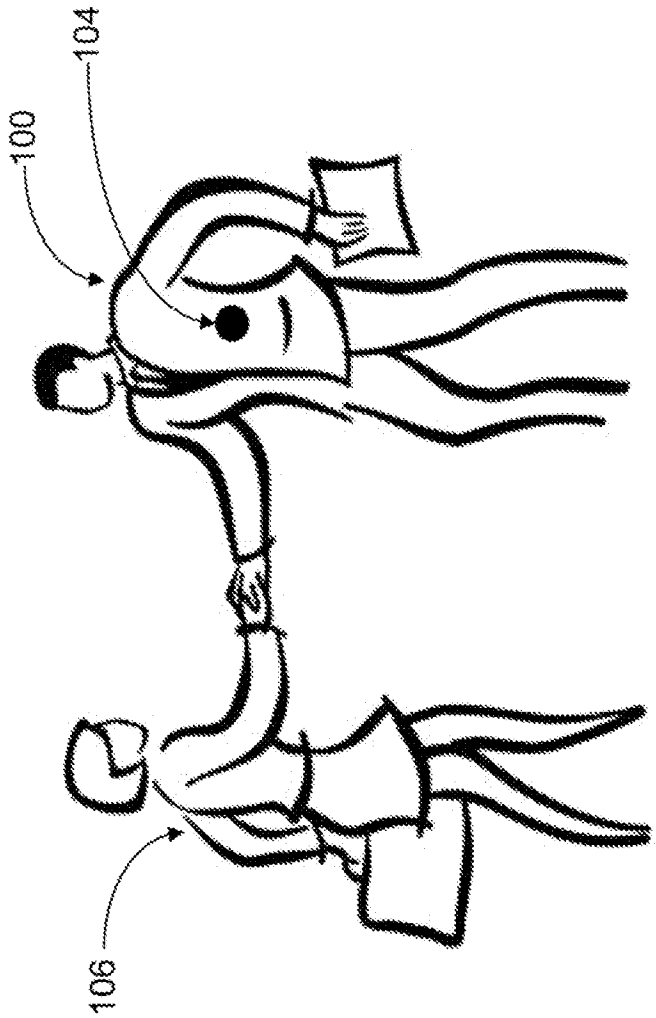


FIG. 1B

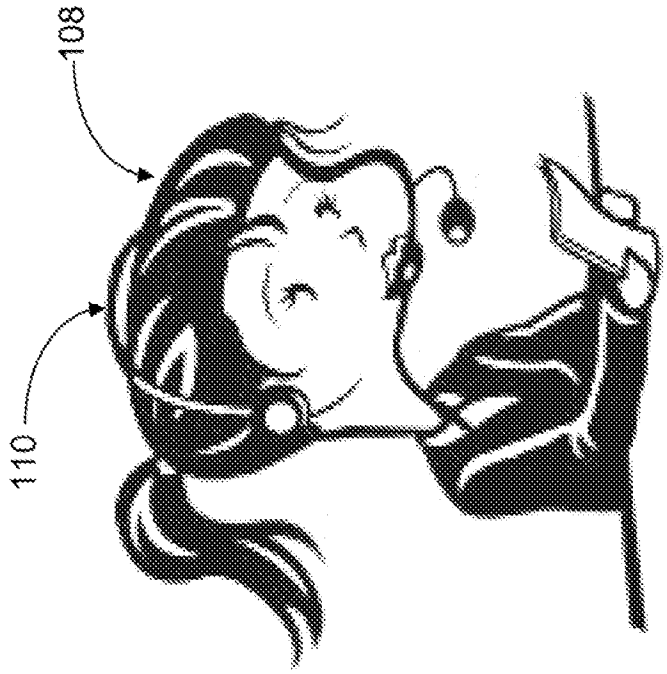


FIG. 1C

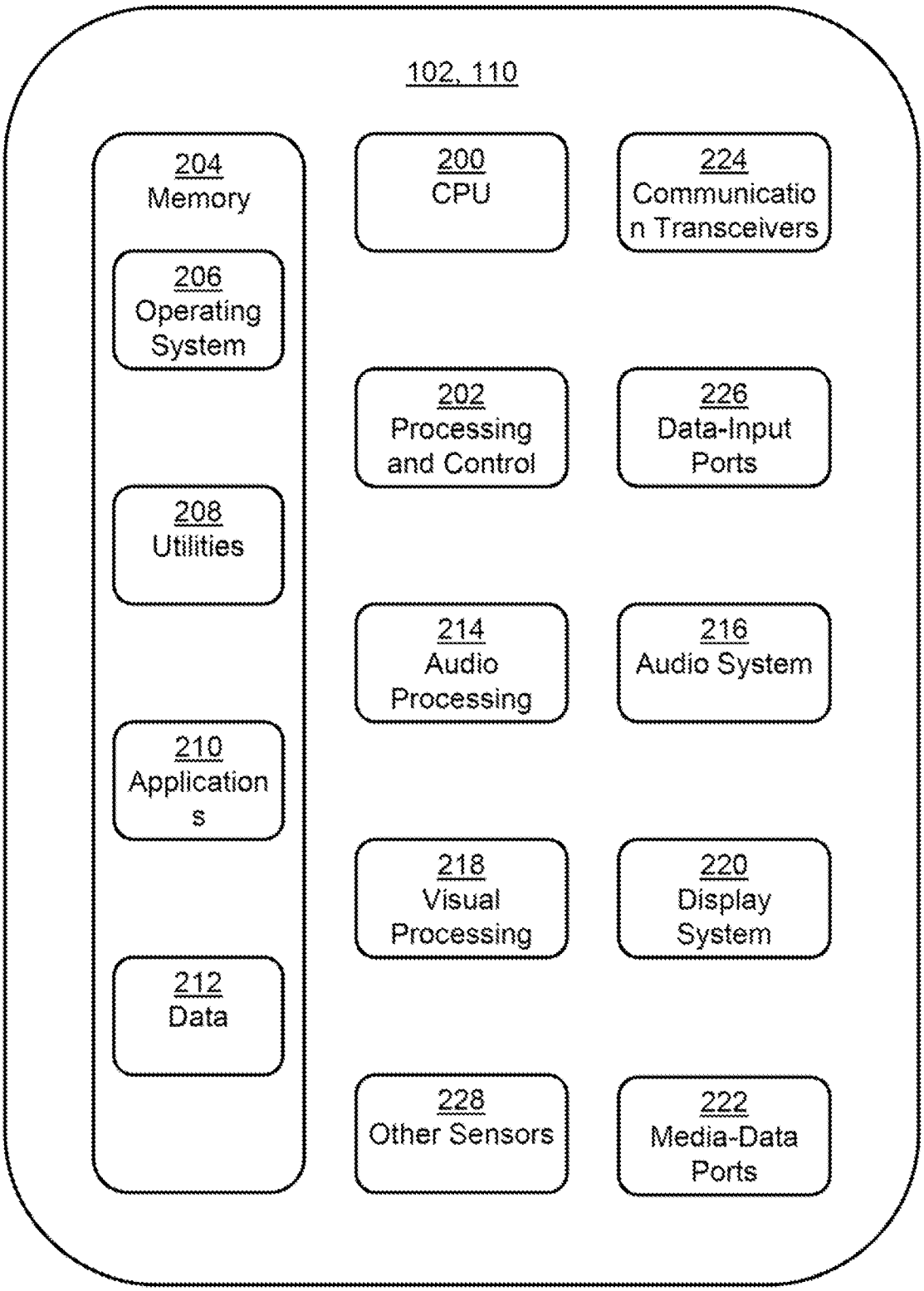

102, 110
204 Memory
206 Operating System
208 Utilities
210 Applications
212 Data
200 CPU
202 Processing and Control
214 Audio Processing
218 Visual Processing
228 Other Sensors
224 Communication Transceivers
226 Data-Input Ports
216 Audio System
220 Display System
222 Media-Data Ports

FIG. 2

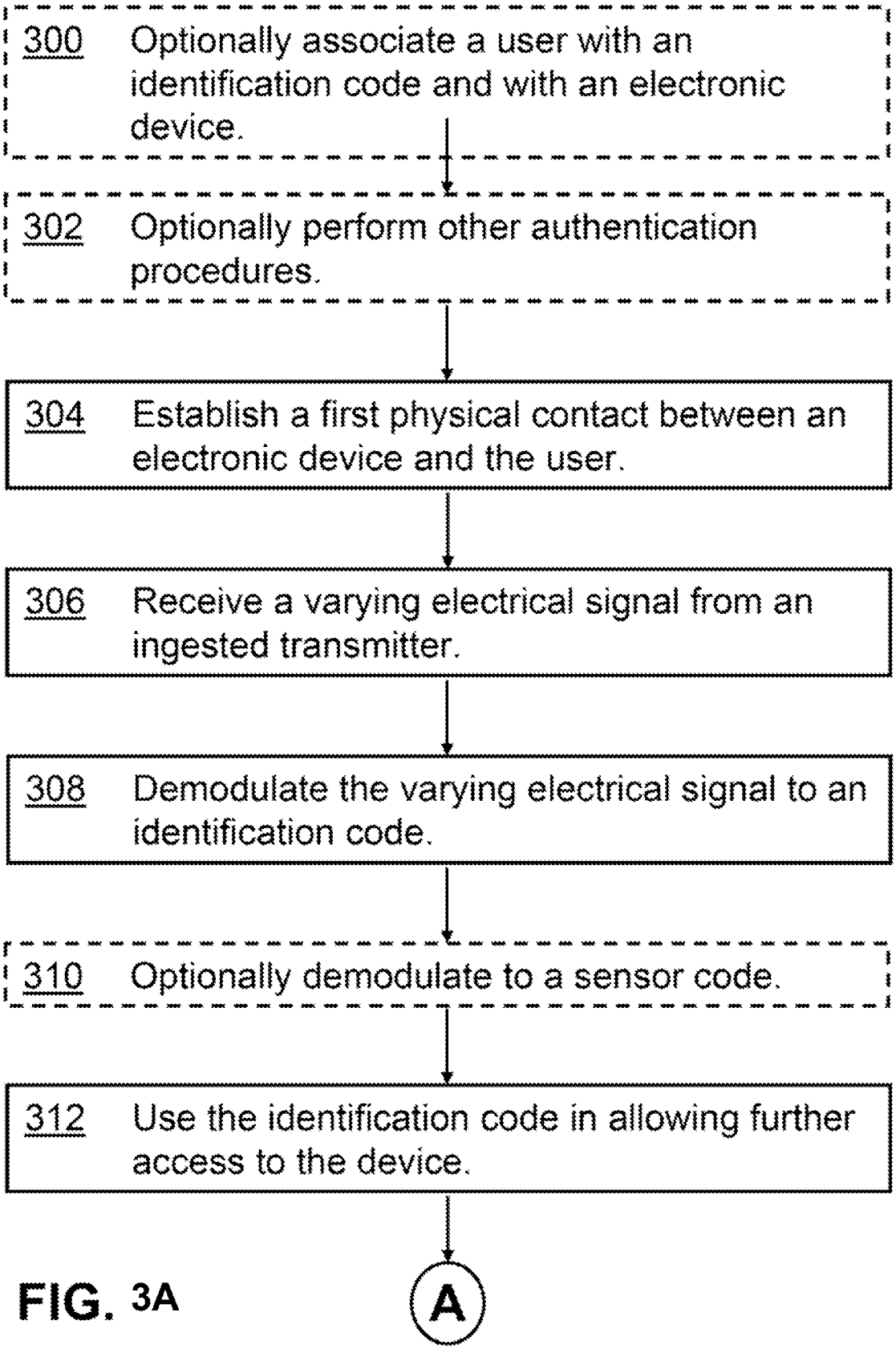

300 Optionally associate a user with an identification code and with an electronic device.
302 Optionally perform other authentication procedures.
304 Establish a first physical contact between an electronic device and the user.
306 Receive a varying electrical signal from an ingested transmitter.
308 Demodulate the varying electrical signal to an identification code.
310 Optionally demodulate to a sensor code.
312 Use the identification code in allowing further access to the device.
A

FIG. 3A

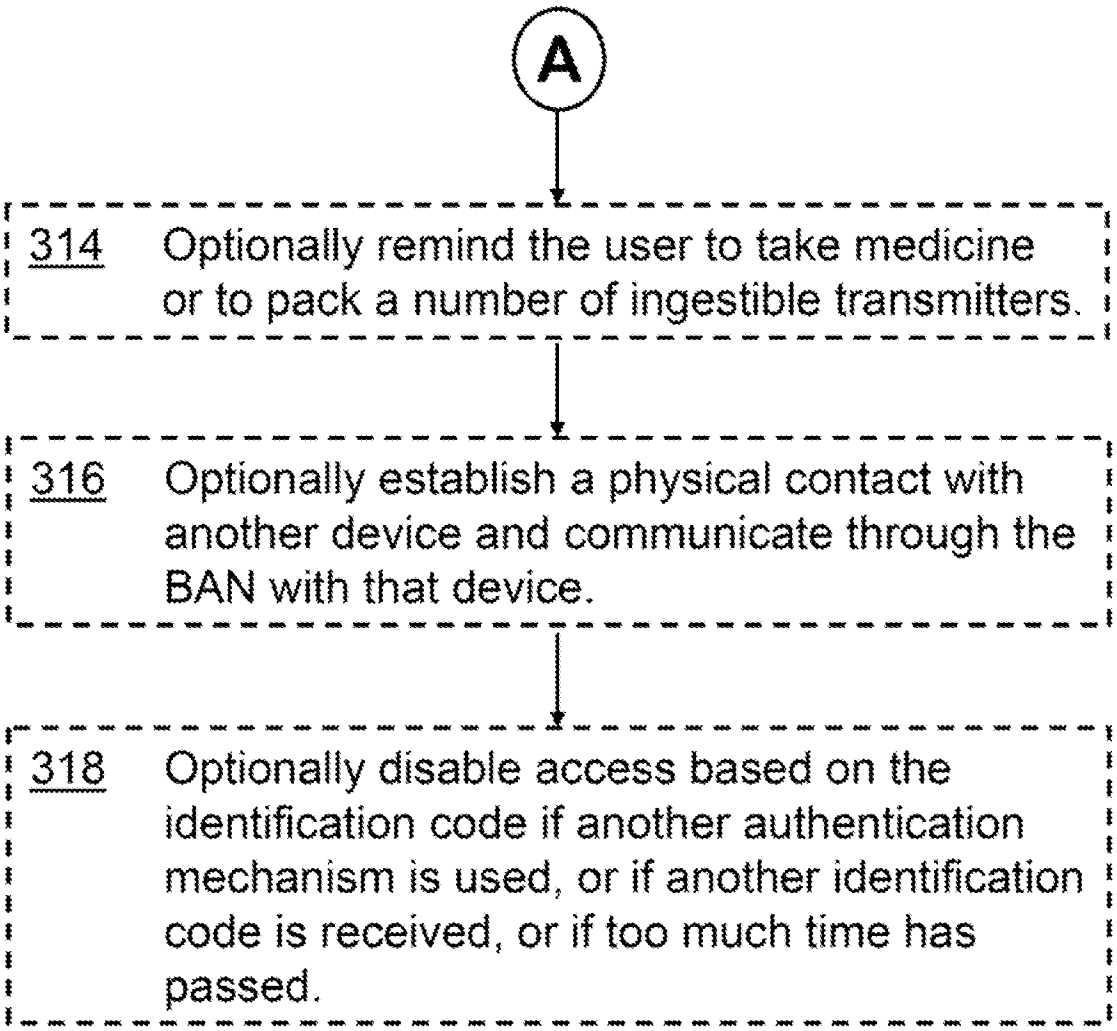

A
314 Optionally remind the user to take medicine or to pack a number of ingestible transmitters.
316 Optionally establish a physical contact with another device and communicate through the BAN with that device.
318 Optionally disable access based on the identification code if another authentication mechanism is used, or if another identification code is received, or if too much time has passed.

FIG. 3B

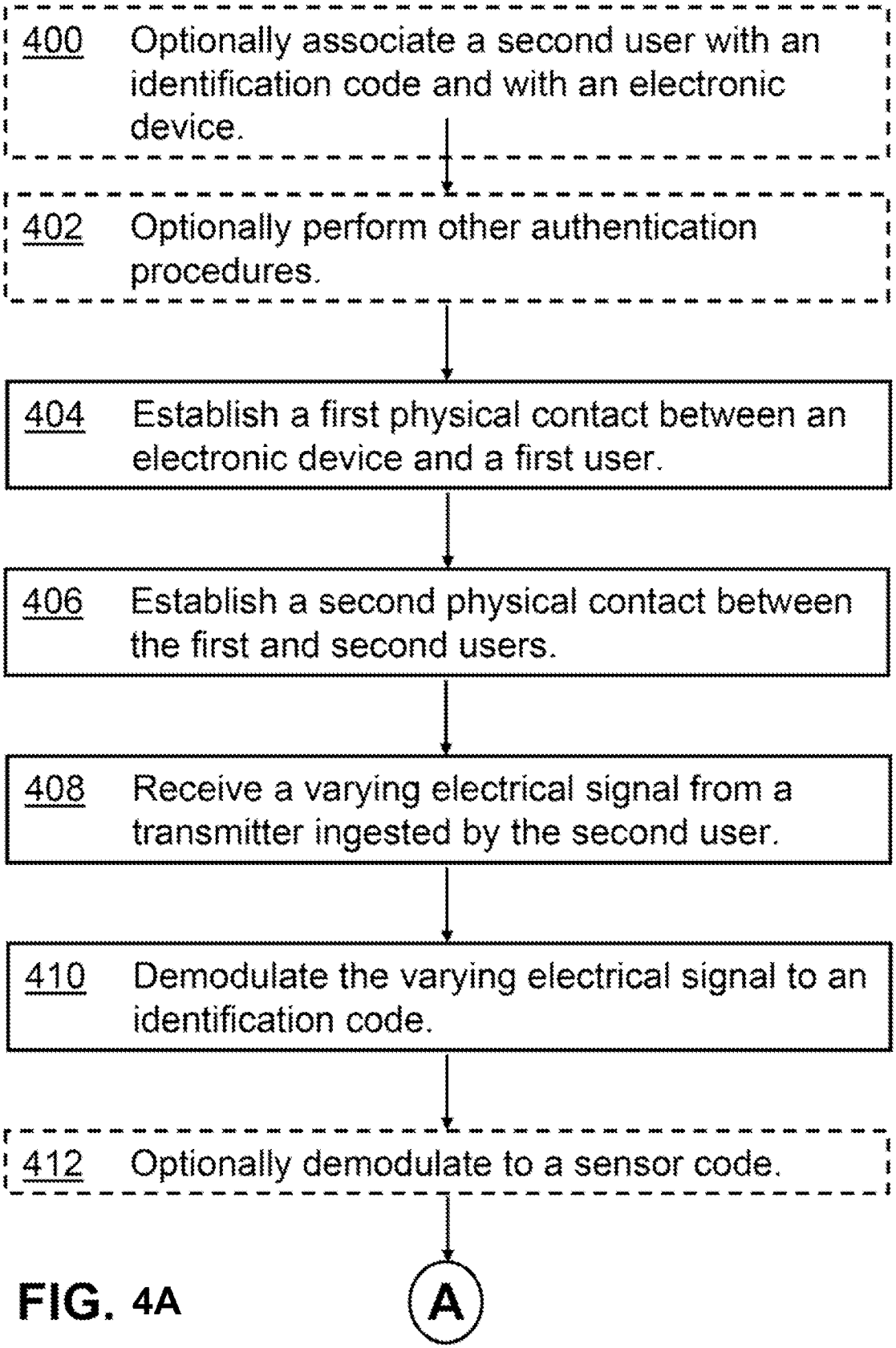

400 Optionally associate a second user with an identification code and with an electronic device.
402 Optionally perform other authentication procedures.
404 Establish a first physical contact between an electronic device and a first user.
406 Establish a second physical contact between the first and second users.
408 Receive a varying electrical signal from a transmitter ingested by the second user.
410 Demodulate the varying electrical signal to an identification code.
412 Optionally demodulate to a sensor code.
A

FIG. 4A

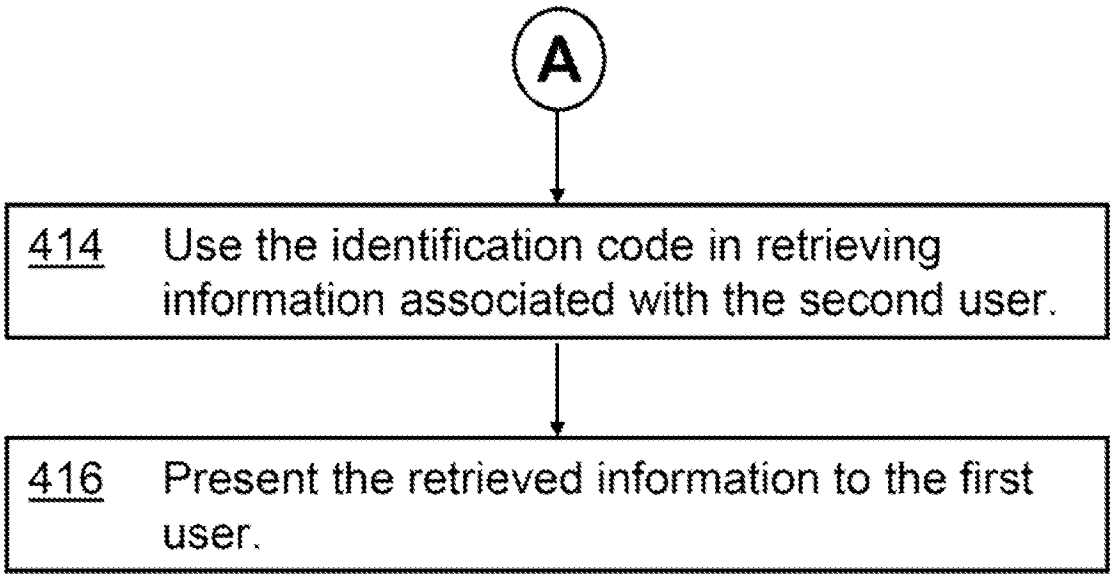

A
414 Use the identification code in retrieving information associated with the second user.
416 Present the retrieved information to the first user.

FIG. 4B

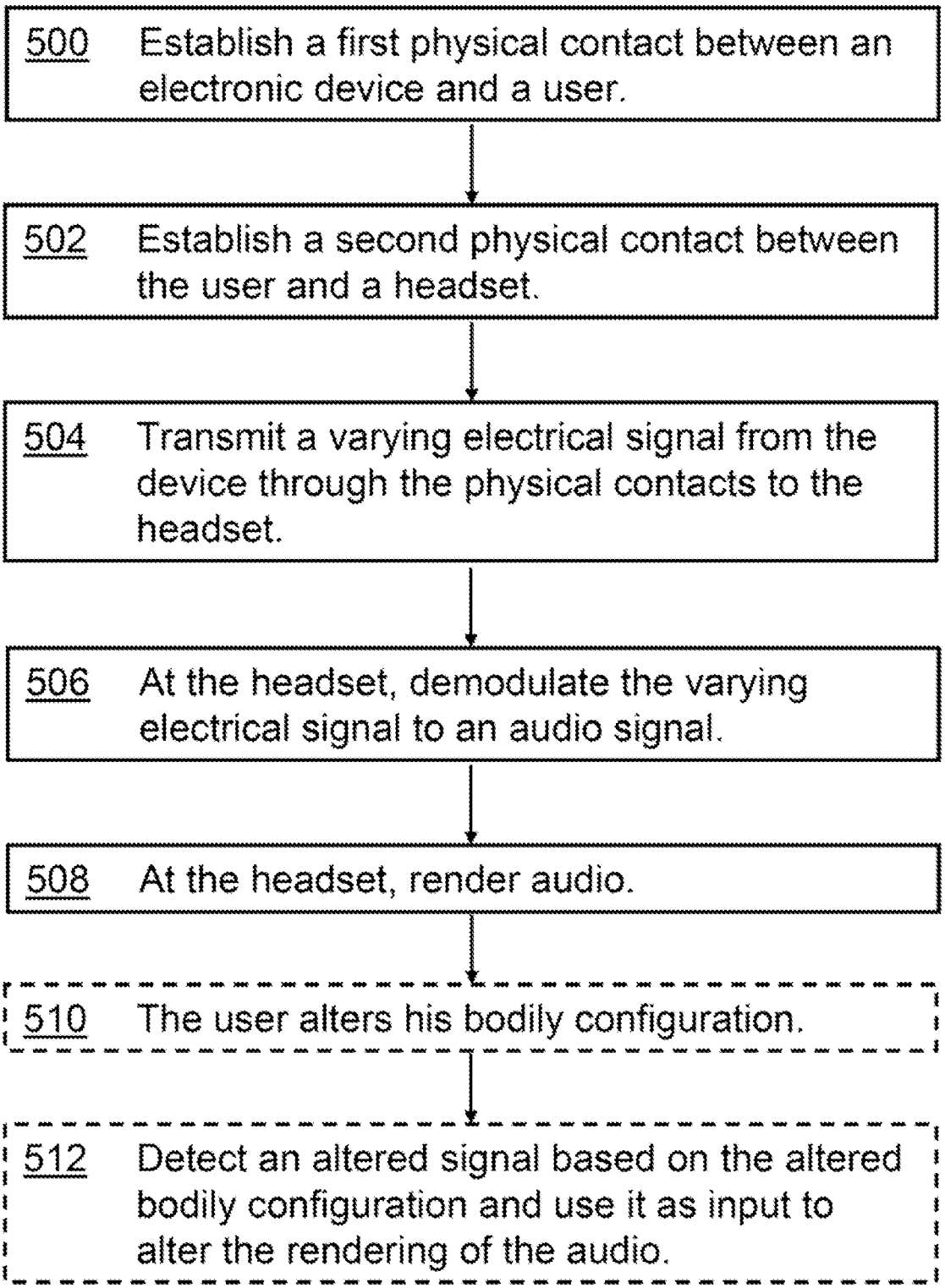

500 Establish a first physical contact between an electronic device and a user.
502 Establish a second physical contact between the user and a headset.
504 Transmit a varying electrical signal from the device through the physical contacts to the headset.
506 At the headset, demodulate the varying electrical signal to an audio signal.
508 At the headset, render audio.
510 The user alters his bodily configuration.
512 Detect an altered signal based on the altered bodily configuration and use it as input to alter the rendering of the audio.

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/015012

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M1/60 H04B13/00
ADD.

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)
H04M H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/202339 A1 (O'BRIEN WILLIAM D [US] ET AL O'BRIEN JR WILLIAM D [US] ET AL) 14 October 2004 (2004-10-14) abstract figures 1,-2,5-6 paragraph [0002] - paragraph [0004] paragraph [0005] - paragraph [0011] paragraph [0034] - paragraph [0050] -----	1-10
X	WO 96/23373 A1 (HAYNES PHILIP ASHLEY [GB]) 1 August 1996 (1996-08-01) abstract page 1, line 1 - line 14 page 1, line 20 - page 3, line 25 page 4, line 9 - line 22 page 7, line 19 - page 9, line 4 figure 1 ----- -/--	1-10

[X] Further documents are listed in the continuation of Box C.

[X] 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
8 April 2014	15/04/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kim-Mayser, Michael

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/015012

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2007 006420 A (MATSUSHITA ELECTRIC WORKS LTD) 11 January 2007 (2007-01-11) abstract ----- ZIMMERMAN T G: "PERSONAL AREA NETWORKS: NEAR-FIELD INTRABODY COMMUNICATION", IBM SYSTEMS JOURNAL, IBM CORP. ARMONK, NEW YORK, US, vol. 35, no. 3/04, 1 January 1996 (1996-01-01), pages 609-617, XP000635090, ISSN: 0018-8670 the whole document -----	1-10
A		1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/015012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004202339 A1	14-10-2004	AU 2004229638 A1	28-10-2004
		CA 2521646 A1	28-10-2004
		EP 1627549 A2	22-02-2006
		US 2004202339 A1	14-10-2004
		WO 2004093486 A2	28-10-2004
WO 9623373 A1	01-08-1996	AT 196044 T	15-09-2000
		AU 712988 B2	18-11-1999
		AU 4492796 A	14-08-1996
		CA 2216416 A1	01-08-1996
		DE 69610075 D1	05-10-2000
		DE 69610075 T2	12-04-2001
		EP 0806099 A1	12-11-1997
		ES 2152008 T3	16-01-2001
		JP H10513021 A	08-12-1998
		US 6118882 A	12-09-2000
		WO 9623373 A1	01-08-1996
JP 2007006420 A	11-01-2007	NONE	