



(86) **Date de dépôt PCT/PCT Filing Date:** 2007/03/20

(87) **Date publication PCT/PCT Publication Date:** 2008/01/17

(45) **Date de délivrance/Issue Date:** 2016/08/16

(85) **Entrée phase nationale/National Entry:** 2008/09/19

(86) **N° demande PCT/PCT Application No.:** US 2007/007288

(87) **N° publication PCT/PCT Publication No.:** 2008/008101

(30) **Priorités/Priorities:** 2006/03/20 (US60/783,785);
2006/03/28 (US60/788,084); 2006/04/16 (US60/792,571);
2006/04/16 (US60/792,570); 2006/05/18 (US60/801,634);
2006/06/14 (US60/813,402); 2006/11/30 (US60/861,917);
2006/12/29 (US60/877,998)

(51) **Cl.Int./Int.Cl. H04M 1/00** (2006.01)

(72) **Inventeurs/Inventors:**

BLACK, GERALD R., US;
BLACK, ALYSSA S., US

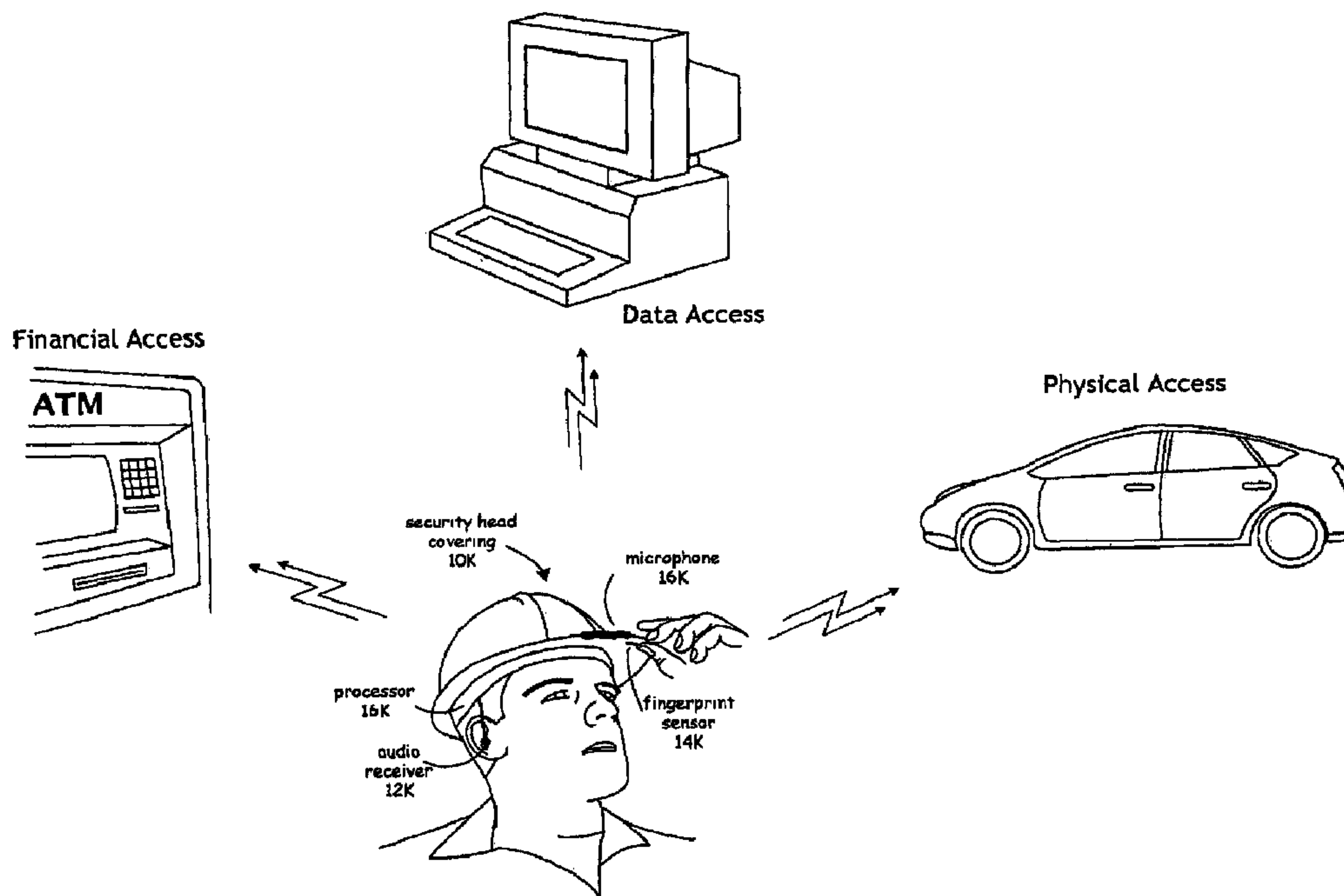
(73) **Propriétaire/Owner:**

BLACK, GERALD R., US

(74) **Agent:** BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.

(54) **Titre : DISPOSITIF DE COMMUNICATION MOBILE**

(54) **Title: MOBILE COMMUNICATION DEVICE**



**FINGERPRINT SECURITY THROUGH A
HEADSET IN A HEAD COVERING**

(57) **Abrégé/Abstract:**

The mobile communication device is for use as a cell phone, as a wireless identity authentication device with other electronic devices, and as a headset in the form of an earphone, an eye-covering, or a head covering for audio communication with a central

(57) Abrégé(suite)/Abstract(continued):

processor, another mobile terminal a cell phone, or a pda. The mobile communication device is hands-free being worn on or near the face, and only requires a finger touching for bimodal identity authentication. An audio receiver is compatible with the ear of the user and a microphone transmits words spoken by the user, electronically there through. A fingerprint sensor is mounted and positioned within th device. When user authentication is required, the user is prompted to touch the fingerprint sensor, and said fingerprint data is compare with fingerprint images of authorized users.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
17 January 2008 (17.01.2008)

PCT

(10) International Publication Number
WO 2008/008101 A3

(51) International Patent Classification:
H04M 1/00 (2006.01)

(74) Common Representative: **BLACK, Gerald, R.**; 30320 Southfield Road #67A, Southfield, MI 48076 (US).

(21) International Application Number:
PCT/US2007/007288

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 20 March 2007 (20.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/783,785	20 March 2006 (20.03.2006)	US
60/788,084	28 March 2006 (28.03.2006)	US
60/792,570	16 April 2006 (16.04.2006)	US
60/792,571	16 April 2006 (16.04.2006)	US
60/801,634	18 May 2006 (18.05.2006)	US
60/813,402	14 June 2006 (14.06.2006)	US
60/861,917	30 November 2006 (30.11.2006)	US
60/877,998	29 December 2006 (29.12.2006)	US

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant and

(72) Inventor: **BLACK, Gerald, R.** [US/—]; 30320 Southfield Road #67A, Southfield, MI 48076 (US).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **BLACK, Alyssa, S.** [US/US]; 148 Lafayette Ne #5, Grand Rapids, MI 49503 (US).

Declaration under Rule 4.17:

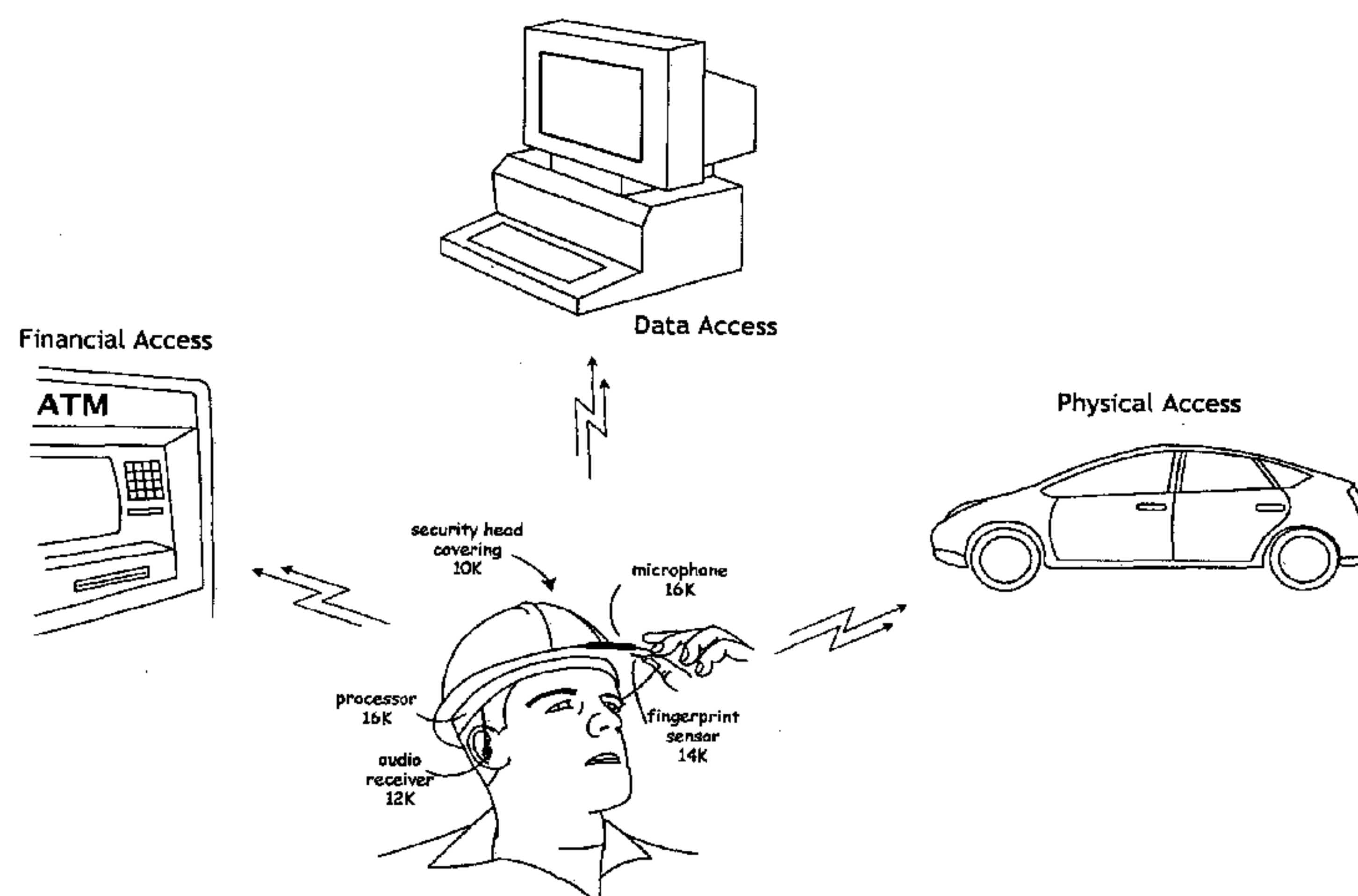
— of inventorship (Rule 4.17(iv))

Published:

— with international search report

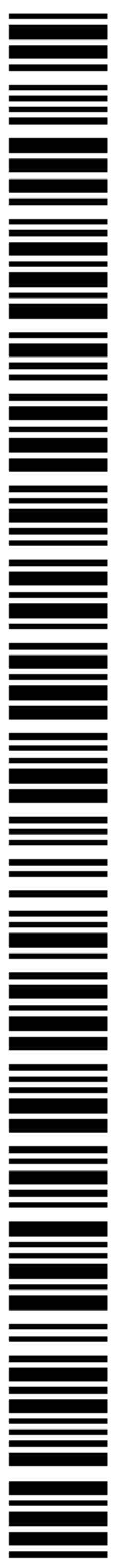
[Continued on next page]

(54) Title: MOBILE COMMUNICATION DEVICE



FINGERPRINT SECURITY THROUGH A
HEADSET IN A HEAD COVERING

(57) Abstract: The mobile communication device is for use as a cell phone, as a wireless identity authentication device with other electronic devices, and as a headset in the form of an earphone, an eye-covering, or a head covering for audio communication with a central processor, another mobile terminal a cell phone, or a pda. The mobile communication device is hands-free being worn on or near the face, and only requires a finger touching for bimodal identity authentication. An audio receiver is compatible with the ear of the user and a microphone transmits words spoken by the user, electronically there through. A fingerprint sensor is mounted and positioned within th device. When user authentication is required, the user is prompted to touch the fingerprint sensor, and said fingerprint data is compare with fingerprint images of authorized users.



WO 2008/008101 A3

WO 2008/008101 A3



— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 April 2008

MOBILE COMMUNICATION DEVICE

FIELD OF USE

The invention involves a mobile communication device that is dual purpose for use with a head set of a cell phone or pda, or as a stand-alone unit, and more particularly, as a hands-free mobile communication device is for use with to gain access to the most secure physical, financial, and data access.

BACKGROUND OF THE INVENTION

In recent years, we have witnessed exponential growth in the penetration rate of mobile telephones and personal digital assistants. The automobile was one of the first environments to become widely populated by cell phones beyond the home and office, allowing people to keep in touch while on the move, or while stuck in traffic. Due to the obvious dangers of holding a cell phone in one hand and driving with the other, many regions of the world either strongly recommend or legally enforce hands-free telephone operation in all moving vehicles. It is now illegal to use a handset while driving.

If a user is performing a task that requires both hands, then the user may not be able to interact with a device to receive a communication. For example, if a parent is grocery shopping with small children, the parent may not be able to handle a mobile telephone to answer an incoming call. Similarly, if a mobile telephone is carried in a purse or a backpack, the user may not be able to locate and answer the telephone before the caller hangs up, particularly if the user is also driving a vehicle. Furthermore, the use of a headset may allow a user to perform such applications without necessarily remaining stationary. Hands-free technology also allows users to multi-task in comfort, resulting in increased effectiveness and productivity.

We are becoming increasingly dependent upon computers to store and access data that affects our lives. Computers are able to remotely access time-sensitive information, on or near a real-time basis from the Internet. It is now essential that a user have access to computer data while at all times.

Currently, phone technology has is the wireless device of choice and many other technologies (e.g. - cameras, smart-phones, Internet connections) are being made compatible with the cell phone.

Some cell phones provide hands-free units that permit the user to talk without having to hold the handset. However, even with the hands-free unit, the user must still dial the phone number or speak the phone number to initiate the call. In general, speech-recognition technology comprises a mechanism for receiving an input voice signal, comparing the input voice signal with stored voice signals, and determining if the input voice signal is sufficiently similar to any of the stored voice signals. If there is a match between the input and stored voice signals, instructions or other data is generated by the device.

In the state-of-the-art headsets the loudspeakers, microphones and communications transceiver devices are combined to a single headset device which is then attached to the user's ear. In cordless and portable headset equipment only compact headset types that are mounted on one ear are able to meet the high requirements set by the user in regard to comfort and user friendliness.

A wearable computer provides the user with perfect recall of previously collected information. Rather than attempting to emulate human intelligence in the computer, wearable computing aims to produce a synergistic combination of human and machine, in which the human performs tasks that it does better, while the computer performs tasks that it does better. Wearable computing affords mobility, personal empowerment, and the freedom from the need to be connected by wire to a communications line. U.S. Patent 7,150,526 (Jannard) discloses wireless interactive headset in the shape of eyeglasses. And, U.S. Publication No. 20040204207 (Parker) discloses a hat, or baseball cap, modified to include a removable headset having a speaker and microphone and a rear mounted pocket holding a cell phone. And, U.S. Publication No. 20050116811 (Eros et al.) discloses a bracelet that the individual wears of a verification signal sent by a central computer unit.

Looking at some other biometric technology, U.S. Patent 6,325,285 (Baratelli) discloses a smart card with integrated fingerprint reader. The sensing surface of the smart card is located such that a user's thumb is naturally positioned over the sensing surface when the card is inserted into a suitable card reader. U.S. Patent 7,088,220 (Kotzin) discloses a wireless communication

device using a plurality of biometric sensors for assessing the identity of a user requesting access to a feature or service provided via the wireless communication device.

What is needed is a device that is ubiquitous to the user that readily carried and located when needed, that comes in a variety of fashions, and can be carried by the user that is compatible with a cell phone or a computer-based wireless communications device, which has become the platform for a broad range of wireless technologies.

What is needed is a device that can confirm the identity of the user in the most secure of all user applications involving either financial security, physical security, or data security, confirming irrefutably the identity of the user, providing bimodal or even multimodal biometric authentication, while enabling the convenience of the use of both hands at all times except when submitting such biometric data.

What is needed is a series of multi-purpose headsets for mobile terminals that are ubiquitous to the user to be able to confirm user identity from any of a variety of locations, and use such confirmation to gain physical access, financial access, and data access from any location in a smooth and seamless manner.

What is needed is a wireless identifier device that is a headset, either as a stand-alone unit, with a cell phone, or with a computer-based wireless communications device, that can be worn for long periods of time with minimal discomfort to the user, that can provide fingerprint certainty for all identity authentication, the sensor being small, rugged, and inexpensive, the terminal enabling the person to have use of both hands for driving a car, encourages multi-tasking and enabling a user to access the most personal records from essentially any location.

SUMMARY OF THE INVENTION

The most fundamental issue in the mobile communication devices of the present invention is that of personal empowerment controlled by the wearer. The mobile communication devices of the present invention are hands-free systems that (1) do not require encumbering wires, (2) can be embedded into existing products worn on the head or about the face, (3) are phone-centric, use speech-recognition technology, and are easy to use, (4) can readily accept a user fingerprint sensor embedded into the device, (5) and can be used in a wide range of applications.

The dual-purpose mobile communication devices of the present invention are integrated into headsets; eye-coverings, such as prescription eyeglasses, sunglasses, or sports goggles; or head-coverings, such as a baseball cap, a civilian hard hat, a football helmet, a hoodie, or any other civilian head covering with a bill that is worn near the mouth of the wearer and can be used as a cell phone or computer-based wireless communications device, as a communication device with another terminal, or as a mobile computer terminal for audio communication with a central processor. The terminal device can operate as a stand-alone unit or with a cell phone, or computer-based wireless communications device. The mobile communication device of the present invention can also be used as a wireless identity authentication device with other electronic devices, such as cell phones, computers, or ATM's.

A fingerprint sensor is embedded or mounted onto the device. When user authentication is required, the user can be prompted to touch the fingerprint sensor. Initially, a person who needs to be authorized to use the terminal submits user data in a registration process. Reference biometric prints are captured during the registration prints, the biometric prints preferably being voice prints, and finger and thumb prints for both hands. Then, subsequently, when the person tries to either transmit or receive signals through the terminal, a sensor in the terminal captures a biometric of the voice, finger, or thumb, and compares such reading against the reference prints of authorized users. If and only if the prints match, user authentication is enabled. If the prints do not match, access is denied.

Multimodal authentication is preferred since the use of more than one authenticating factor decreases the likelihood of false positives, that is, the likelihood of an unauthorized user gaining access. The fingerprint is initially used, and the voiceprint is used for confirmation. Alternatively, multiple fingerprint images can be captured. Also, voice recognition is used to confirm the identity of the person wearing the headset.

In the preferred embodiment of the headset of the present invent, the headsets are "on" essentially all the time during the business day providing each user with full agility and mobility while in continuous audio communication. The headset enables each agent to have both hands free, which is needed for processing passengers.

The mobile communication device of the present invention is any device that includes memory and processing power, that has access to a central processing unit including memory and means for delivering data (computer screen, audio receiver) to the user, and means for the user to enter data (audio transmitter, keypad, camera, touch sensitive screen) to the central processing unit, such devices including but not limited to cell phones, cordless phones, conventional wired phones, tethered phones, cordless phones, walkie-talkies, handheld computers, personal digital assistants, pen-based computers, remote controls, smart phones, and similar-type device.

The mobile communication device of the present invention affords and requires mobility, and the freedom from the need to be connected by wire to an electrical outlet, or communications line. Rather than attempting to emulate human intelligence in the computer, as is a common goal of research in Artificial Intelligence, the goal of these mobile terminals is to produce a synergistic combination of human and machine, in which the human performs tasks that it is better at, while the computer performs tasks that it is better at.

Some of the advantages of the mobile communication device of the present invention is that it is both hands-free and eyes-free; is worn on the ear, face or head; can be easily found when needed; provides fingerprint certainty; can be used for (a) physical access; (b) data access; and (c) financial access; uses durable sensors that are compatible with other biometric systems; uses inexpensive sensors that are state-of-the-art; is compatible with cell phones, handheld computers, and personal computers; and provides a date-time stamp for all communications.

Short-distance wireless communication technologies are used to transmit data from a sensor to a headset, from a headset to a cellphone, from a headset to computer, or from an identification device to a computer. The wireless communicating based on these communication technologies can establish the cordless communication between devices and terminals, thereby simplifying the device connection work and, at the same time, enhancing convenience because it is substantially unnecessary to select installation spaces of the cordlessly connected devices.

To make a call using the mobile communication device of the present invention, the user needs to speak into the microphone the name or number that is sought. Speech-recognition technology is used, much the same as deployed in vehicles. For example, U.S. Publication No. 20050143134 (Harwood et al.) discloses a vehicular, hands-free telephone system. The appliance uses text-to-speech to transfer phonebook entries from the cell phone to memory of the appliance. The

appliance uses text-to-speech to transfer phonebook entries from the cell phone to memory of the appliance. The appliance uses text-to-speech to read and display text messages incoming to the cell phone for the operator to hear and view. The appliance initiates connecting and disconnecting of the cell phone with the appliance in response to voice commands of the operator.

The term "headset", as used herein refers to a mobile communication device for providing sounds into which sound signals output from a sound device are heard by a user, and the voice of the user is converted into electrical signals, the headset being either a stand-alone unit, in digital communication with another headset, a cell phone, or a computer. The headset enables the user to communicate hands-free. The term "cap" as used herein refers to a garment selected by a person to be worn as a fashion statement to cover the head of the person to provide warmth to the head, to protect the head from rain or snow, or to protect the eyes from the sun.

For a more complete understanding of the mobile terminal of the present invention, reference is made to the following detailed description and accompanying drawings in which the presently preferred embodiments of the invention are shown by way of example. Thus, a number of preferred embodiments have been fully described above with reference to the drawing figures. The scope of the claims should not be limited by the preferred embodiments and examples, but should be given the broadest interpretation consistent with the description as a whole.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURES 1A and 1B disclose two preferred embodiments of the mobile communication device of the present invention.

FIGURES 1C, 1D, and 1E disclose three preferred embodiments of the mobile communication device of the present invention in the form of three different eye-coverings.

FIGURES 1F through 1K disclose additional preferred embodiment of the mobile communication device of the present invention in the form factor of various head coverings.

FIGURE 2 is a schematic depicting the mobile communication device of FIGURE 1K being used for financial access, data access, or physical access.

FIGURE 3A discloses the mobile communication device of FIGURE 1B having a short-distance wireless communication with a flip phone.

FIGURE 3B discloses the mobile communication device of FIGURE 1E having a short-distance wireless communication with a pda.

FIGURE 4A discloses the mobile communication device of FIGURE 1C being in short-distance wireless communication with various conventional devices (a wrist screen, an IPOD®, a laptop computer, a handheld computer, a cell phone, a personal computer, and a home entertainment center).

FIGURE 4B discloses a preferred embodiment using a cell phone being in short-distance wireless communication with a plurality of different mobile communication devices of the present invention - a head covering, an eye covering, and a headset.

FIGURE 5 discloses a preferred embodiment of a simplified logic diagram for a registration process for the mobile communication device of either FIGURE 1A or 1B.

FIGURE 6 discloses a preferred embodiment of a simplified logic diagram for an identity confirmation method using the mobile communication device of either FIGURE 1A or 1B.

FIGURE 7A discloses a preferred embodiment of a simplified logic diagram using the mobile communication device of either FIGURE 1A or 1B for wire transferring funds. FIGURE 7B discloses a preferred embodiment of a simplified logic diagram using the mobile communication device of either FIGURE 1A or 1B for the buying stock on the Internet. FIGURE 7C discloses a preferred embodiment of a simplified logic diagram using the mobile communication device of either FIGURE 1A or 1B for currency conversion.

FIGURE 8 discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B for payment processing at a checkout terminal.

FIGURES 9A, 9B, and 9C disclose a shell for a cap-terminal of the present invention, the shell, being compatible with multiple conventional head coverings.

FIGURE 10A discloses a conventional pair of glasses. FIGURE 10B and FIGURE 10C disclose a preferred embodiment of the processor/headset unit of the present invention that is compatible with a wing or the frame, respectively, of the eyeglasses of FIGURE 10A.

FIGURE 11A discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B to access a garage door from inside a vehicle; and FIGURE 11B discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B to access a car door from outside the vehicle.

FIGURES 12A, 12B, and 12C disclose three alternative preferred embodiments of a simplified version of three additional embodiments of the communication device of the present invention, the communication device being deployed as an identification device in a head covering (FIGURE 12A), an ID badge (FIGURE 12B), or an eye-covering (FIGURE 12C).

FIGURE 13A discloses a simplified schematic for using the mobile communication device of either FIGURE 1A or 1B to gain access to an account at an ATM. Similarly, FIGURE 13B discloses a simplified schematic for using the mobile communication device of FIGURE 1B to gain access to a PC or secure data within the PC.

FIGURE 14A discloses the identifier device of the present invention as a head covering, an ID badge, or eyeglasses in direct wireless communication with the handset of a cell phone to identify the user or wearer of such identifier device; and FIGURE 14B discloses the identifier device of the present invention as a head covering or eyeglasses in direct wireless communication with the headset, the headset then being in direct wireless communication with a handset of a cell phone for purposes of identifying the user or wearer of such device.

FIGURE 15A discloses a simplified schematic of another preferred embodiment of the mobile communication device of the present invention used as an identifier device; and FIGURE 15B discloses a simplified schematic of the preferred embodiment of the mobile communication device of the present invention in a wearable computer. FIGURE 15C depicts a simplified logic diagram for speech recognition using the mobile communication device of FIGURE 1A or 1B, the user speaking commands to the microphone that are used for purposes of completing a phone call, for example.

FIGURE 16A discloses a simplified block diagram of a personal terminal-based security system; FIGURE 16B discloses a simplified block diagram of a corporate terminal-based security system; FIGURE 16C discloses a simplified block diagram of a resort or luxury cruise terminal-based security system; FIGURE 16D discloses a simplified block diagram of a hospital terminal-based security system; and FIGURE 16E discloses a simplified block diagram of a law-enforcement terminal-based security system, each deploying one of the mobile communication devices of FIGURE 1A through 1K.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to the drawings, FIGURES 1A and 1B disclose two preferred embodiments of the mobile communication device (10A and 10B) of the present invention. The mobile communication device is a headset that is worn on the ear of a user. During routine usage, the units are hands-free, and only require a finger touch or sweep to authenticate the identity of the wearer.

The mobile communication device 10A of FIGURE 1A is similar in appearance to a Plantronic Discovery™ 655 headset, and the mobile communication device 10B of FIGURE 1B is similar in appearance to a Nokia HDW-3 wireless headset. Each communication device includes an audio receiver (12A and 12B), a microphone (15A and 15B), and a processor (16A and 16B).

The core of the mobile communication device of the present invention is a fingerprint sensor (14A and 14B respectively) enabling the person wearing the headset to authenticate user identity. The fingerprint sensor is commercially available from Authentec. If an area sensor is to be used (as shown), the MBF 200 is commercially available from Fujitsu of Japan, and the FPC1010 is commercially available from Fingerprint Cards AB of Gothenburg, Sweden. If a sweep sensor is used, the sensor of choice is either the Entrépad 1510 or the Entrépad 2510. The fingerprint is generally submitted upon response to a system prompt submitted to the wearer through the audio receiver. Another sweep sensor of choice is manufactured by Atmel, the AT77C104, the FingerChip having integrated navigation. The fingerprint sensor (14A or 14B) not only protects the phone and its stored information, but enables operators to provide new, profitable services such as mobile commerce and wireless banking. The sensor also allows manufacturers to easily add new features like gaming navigation, touch menu scrolling, multi-

finger speed dialing, hot key application launch, favorite song and photo recall, and others that differentiate the phone and improve the user experience.

The mobile communication device 10A of FIGURE 1A includes a power source 18A and is a self-contained unit. The power source 18A is a battery and provides power to the microphone 15A and the audio receiver 12A. The battery can be replaced or recharged. The mobile communication device of FIGURE 1B is a headset for use with a cell phone, a computer, or a pda.

FIGURES 1C, 1D, and 1E disclose three preferred embodiments of the dual-purpose mobile communication device of the present invention (10C, 10D, and 10E) in the form of three different eye-coverings. The mobile communication device 10C of FIGURE 1C is a pair of eyeglasses with corrective lenses. The mobile communication device 10D of FIGURE 1D is a pair of sports goggles. The goggles can be used for bicycling, hand-gliding, mountain climbing, and the like. The mobile communication device 10E of FIGURE 1E is a pair of sunglasses. Each eye-covering includes an audio receiver (12C, 12D, and 12E), a microphone (15C, 15D, and 15E), and a processor (16C, 16D, and 16D), and each mobile communication device includes a fingerprint sensor (14C, 14D, and 14E). The fingerprint sensor (14C, 14D, and 14E) enables the wearer of the eye-covering to authenticate user identity, the fingerprint generally being submitted upon response to a system prompt submitted to the wearer through the audio receiver (12C, 12D, and 12E). According to the invention, the microphone 15C, 15D, and 15E is preferably an ultra flat high-sensitivity one, preferably embedded on the underside of the lens and hidden, and facing the wearer. Electronic noise-reduction components to filter wind-generated noise from an audio signal transmitted from the microphone (not shown), are also located inside the frame, as well as suitable electrical connections. Electrical contacts for continuity must be provided at a corresponding hinge. As a result of the symmetry of the eye-coverings, the audio receivers (12C, 12D, and 12E) can be deployed for each ear, enabling the wearer to use the mobile communication device to play stereophonic sound for listening to music.

FIGURES 1F, 1G, and 1H disclose additional preferred embodiment of the dual-purpose mobile communication device of the present invention (10 F, 10G and 10H) in the form of head coverings, wherein each mobile communication device is used to confirm the identity of the wearer. The mobile communication device 10F of FIGURE 1F is in the form of a baseball cap, whereas FIGURES 1G and 1H disclose alternative head-covering designs. In each, a microphone (15F, 15G, and 15H) is positioned as an audio pickup in the bill of the head covering, which picks

up words spoken by the wearer. Two sweep fingerprint sensors (14F, 14G, and 14H) are positioned on the underside of each bill, one sensor for each hand. As a result of the symmetry of the head covering, there are audio receivers for each ear, enabling the wearer to use the mobile communication device to hear music in each ear, which is optional.

FIGURES 1I discloses another preferred embodiments of the dual-purpose mobile communication device of the present invention 10I, the mobile communication device being a security head covering. The mobile communication device is a head-covering hoodie 10I, such that adults can communicate with and locate teenagers, and also teenagers can communicate with each other via closed circuit or "walkie-talkie" or conventional cell phone lines on outdoor excursions. A cell phone or a computer-based wireless communications device can be carried in a pocket and wired to the audio receivers and microphone through the garments. Each garment includes an audio receiver 12I, a microphone 15I, and a processor 16I, and each mobile communication device includes a fingerprint sensor 14I. A global-positioning sensor 19I is used to locate the wearer, and the garment includes a power source 18I. The symmetry of the garment enables audio receivers for each ear, so that the wearer can use the mobile communication device 10I to listen to music.

Having a wearable computer on the face or as a head covering has much utility for people in outdoor applications particularly, with the GPS sensor, and even without the biosensor. For example, a scout leader can maintain two-way communications continually with a group of scouts on an outdoor, overnight field trip. The scout leader equips each of the individual scouts with headsets with the GPS sensor. In the event that one or more scouts get lost, hurt, or otherwise separated from the main unit, the headset is an invaluable device for locating the separated scout or scouts.

FIGURE 1J discloses yet another preferred embodiment of the dual-purpose mobile communication device of the present invention 10J, the mobile communication device embedded in a football-helmet. Each helmet includes an audio receiver 12J, a microphone 15J, and a processor 16J, and each mobile communication device 10J includes a fingerprint sensor 14J. Each helmet includes a GPS sensor 19J and a power source 18J. The fingerprint sensor enables secure communications between the coaches and the quarterback, since a match is

required before the audio signals are received by the quarterback. A sweep fingerprint sensor is shown.

FIGURE 1K discloses yet another preferred embodiment of the dual-purpose mobile communication device of the present invention 10K, the mobile communication device 10K being embedded in a civilian hardhat, the type typically used in building construction. Each helmet includes an audio receiver 12K, a microphone 15K, and a processor 16K, and each mobile communication device 10K includes a fingerprint sensor 14K, a sweep fingerprint sensor being preferred. Again, dual audio receivers are preferred.

FIGURE 2 is a schematic depicting the mobile communication device of FIGURE 1L being used for financial access, data access, or physical access by spoken communications with the designated gatekeepers. The dual-purpose communication device of the present invention enables biometric authentication of a user, said dual-purpose communication device being digitally connected to a communications system. The dual-purpose communication device can be a headset, a head covering, or an eye-covering. A processor is positioned with the communication device, and is in electrical communication with the fingerprint sensor in the communication device. A short-distance wireless communication device that is compatible with the processor positioned in the dual-purpose communication device of the present invention. The short-distance wireless communication device enables the retrieval of fingerprint data from a processor within the dual-purpose communication device. The biometric authentication is determined by another processor; said other processor being external to said dual-purpose communication device and is based at least in part upon a comparison of the sensed fingerprint data and reference fingerprint data of at least one authorized user. If the print in the communication device matches a reference print, eventually authentication will need to be confirmed with reference prints in the headset, cell phone, or master computer before authentication can be confirmed.

FIGURE 3A discloses a yet still another preferred embodiment of the mobile communication device of the present invention, the mobile communication device 10B, the mobile communication device 10B being in a short-distance wireless communication with a flip phone 20A. The flip phone 20A includes a data entry keypad 28A and a display screen 24A. FIGURE 3B discloses another preferred embodiment of the present invention deploying a mobile communication device 10E, the mobile communication device 10E being deployed as a headset

for use with a pda 20B. The pda 20B includes a data entry keypad 28B and a display screen 24B. Short-distance wireless communication technologies can be used to transmit data from the mobile communication device to the cell phone. The wireless communicating based on these communication technologies can establish the cordless communication between devices and terminals, thereby simplifying the device connection work and, at the same time, enhancing convenience because it is substantially unnecessary to select installation spaces of the cordlessly connected devices. However, wired connections can also be deployed.

FIGURE 4A discloses the mobile communication device of the present invention as pair of sunglasses, the mobile communication device having Bluetooth® compatibility with various conventional devices (a wrist screen, an IPOD®, a laptop computer, a handheld computer, a cell phone, a personal computer, and a home entertainment center), the mobile communication device including a biosensor for identity authentication, an audio transmitter in the visor, either one or two audio receivers near the ears, preferably enabling plug-in connection with the ear canal(s), and a processor in the underside of the visor. By having the identity authentication in the headset, conventional electronic hardware can provide biometric security. With the exception of the home entertainment center, these connections can also be hard-wired to the mobile communication device of the present invention. Hence, the mobile communication device of the present invention can also be used to access these devices, providing fingerprint security. FIGURE 4B discloses a preferred embodiment using a cell phone that is compatible with a plurality of different mobile communication devices of the present invention, each mobile communication device being a headset and being used by the same or different users, and each mobile communication device providing biometric authentication through the headset.

FIGURE 5 discloses a preferred embodiment of a simplified logic diagram for a registration process for the mobile communication device of the present invention of either FIGURE 1A or 1B, the pertinent data being submitted manually by the Applicant. Initially, a person authorized to use the terminal is registered through a registration process. Reference biometric prints are captured during the registration, the prints being voice prints, hand prints (index fingerprint, thumbprints, and palm prints for each hand), and ear prints. The ear print can be a shape of the ear lobe or pinna, a thermal image of the ear pinna, a vein pattern of the ear pinna, the shape of the ear canal, or some other biometric measurement associated with the ear. Then, subsequently, when the person tries to either transmit or receive signals through the terminal, a sensor in the terminal captures a biometric of the voice, hand, or ear, and compares such

reading against the reference prints that are authorized to use the terminal. If and only if the prints match, use of the terminal is enabled. If the prints do not match, the terminal is disabled and no signals can be received or transmitted through said terminal. The issuing authority may be a corporation, a bank, a hospital, or a head-of-household. Preferably, the issuing authority will need to approve the user being added to the system.

FIGURE 6 discloses a preferred embodiment of a simplified logic diagrams for an identity confirmation method using the mobile communication device of either FIGURE 1A or 1B.

FIGURE 7A discloses a preferred embodiment of a simplified logic diagram of a method for wire transferring funds using the mobile communication device of either FIGURE 1A or 1B. The wire transfer is made to an escrow account, which is subsequently transferred to the account of the payee, the escrow account keeping the account number of the payee for purposes of privacy and account security. FIGURE 7B discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B for currency conversion.

FIGURE 8 discloses a preferred embodiment of a simplified logic diagram for a payment processing system using the mobile communication device of either FIGURE 1A or 1B for payment processing at a checkout terminal at a point-of-sale transaction.

FIGURES 9A, 9B, and 9C disclose a shell for a cap-terminal of the present invention, the shell, being compatible with multiple conventional head coverings, the shell including an audio transmitter and an audio receiver, a processor, and preferably a fingerprint sensor. The audio receiver is either for one ear or both ears, two ear reception being needed for listening to music. The audio receiver either covers the ears or is in close enough proximity to the ears that ear plugs are not needed.

FIGURE 10A discloses a conventional pair of glasses. FIGURE 10B discloses a preferred embodiment of the processor/headset unit of the present invention that is compatible with an earpiece of the glasses of FIGURE 10A, the headset unit including an audio transmitter and an audio receiver and a fingerprint sensor. FIGURE 10C discloses another preferred embodiment of a processor/headset of the present invention that is worn above the lenses of the glasses, the headset unit being attachable above the lenses of the glasses, the headset unit including an audio transmitter and an audio receiver, and a fingerprint sensor.

FIGURE 11A discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B to access a garage door from inside a vehicle, the system being bimodal and using fingerprint and voiceprint matching, said prints being submitted during a registration process similar to one shown in FIGURE 5, the user speaking "garage door" which are recognizable words to the system which prompts the system to request the user to submit a voiceprint using the terminal and a fingerprint using the terminal to confirm user identity before completing the processing of the request for opening the garage door.

FIGURE 11B discloses a preferred embodiment of a simplified logic diagram for using the mobile communication device of either FIGURE 1A or 1B to access a car door from outside the vehicle, the system being bimodal and using fingerprint and voiceprint matching, said prints being submitted during a registration process similar to one shown in FIGURE 5, the user speaking "car door" which are recognizable words to the system which prompts the system to request the user to submit a voiceprint using the terminal and a fingerprint using the terminal to confirm user identity before completing the processing of the request for opening the car door.

FIGURES 12A, 12B, and 12C disclose three alternative preferred embodiments of a simplified version of dual-purpose mobile communication device being of the present invention (10Q, 10R, and 10S) for use as an identification device. FIGURE 12A discloses an eye-covering embodiment, FIGURE 12B discloses an ID badge embodiment, and FIGURE 12C discloses a head covering embodiment. Each embodiment includes a fingerprint sensor (14Q, 14R, and 14S) and a processor (16Q, 16R, and 16S), the identification device (10Q, 10R, and 10S) being useful for authenticating the identity of the wearer for subsequent purposes of financial access, data access, or physical access. The processor (16Q, 16R, and 16S) is in electrical communication with the fingerprint sensor (14Q, 14R, and 14S) and compares captured fingerprint data with reference fingerprint data of at least one authorized user to determine if access is authorized.

FIGURE 13A discloses a simplified schematic for using the mobile communication device of either FIGURE 1A or 1B to gain access at an ATM. The on-site prepaid transaction uses the mobile headset terminal of either FIGURE 1A or 1B which includes an RFID. The user at the ATM selects "Enter Remote Fingerprint" and an interrogator at the ATM receives the fingerprint data from the headset. Once the user fingerprint matches the reference fingerprint in the headset, the user fingerprint is compared against an ATM reference fingerprint. Similarly, FIGURE 13B

discloses a simplified schematic for using the mobile communication device of FIGURE 1B to gain access to a PC or secure data within the PC. The user at the PC selects "Enter Remote Fingerprint" and an interrogator at the PC receives the fingerprint data from the headset. Initially, the user's fingerprint is compared against a headset reference fingerprint. If there is a match, then the user's fingerprint is compared against a system or network reference fingerprint template.

FIGURE 14A discloses the identifier device of the present invention as a head covering, an ID badge, or eyeglasses in direct wireless communication with the handset of a cell phone for purposes of identifying the user or wearer of such device.

FIGURE 14B discloses the identifier device of the present invention as a head covering or eyeglasses in direct wireless communication with the headset, the headset then being in direct wireless communication with a handset of a cell phone for purposes of identifying the user or wearer of such device.

FIGURE 15A discloses a simplified schematic of another preferred embodiment of the mobile communication device of the present invention in a head covering or glasses including a biometric sensor, a processor, a two-way RFID tag, a global-positioning sensor, and an interrogator. FIGURE 15B discloses a simplified schematic of the preferred embodiment of the mobile communication device of the present invention in a wearable computer including an audio transmitter, an audio receiver, a biometric sensor, a processor, a two-way RFID tag, a global-positioning sensor, and an interrogator.

FIGURE 15B is a block diagram of depicting the terminal exemplary embodiments of terminal and headsets for using the invention. Specifically, the terminal for communicating with a central computer may comprise processing circuitry, which may include a processor for controlling the operation of the terminal and other associated processing circuitry. The processing circuitry will incorporate audio processing circuits such as audio filters and correlation circuitry associated with speech recognition. In accordance with one aspect of the present invention, the terminal is used in a voice-driven system, which uses speech recognition technology for communication. The headset provides hands-free voice communication between the wearer and the terminal. FIGURE 15B illustrates a simple block diagram of one exemplary embodiment of the present invention. Specifically, FIGURE 15B incorporates a headset, which is configured to communicate

in one aspect on either a wired link or a wireless link with a portable terminal. Alternatively, portable terminal might be a stand-alone system or device that merely communicates with a user through the headset. In still another alternative embodiment, the headset might communicate directly on link to a central computer. FIGURE 15C depicts a simplified logic diagram for speech recognition using the mobile communication device of FIGURE 1A or 1B, the user speaking commands to the microphone that are used for purposes of completing a phone call, for example.

Multispectral Imaging, Inc. is a leader in the design and development of infrared imaging systems, today announced an exclusive worldwide license with Oak Ridge National Laboratory (ORNL) for its patents involving the use of microcantilever sensors for infrared imaging. The company is commercializing unique and proprietary technology that has the potential for radical improvements in both price and performance of uncooled infrared focal plane arrays.

Speaker authentication is also starting to move into call centers. As with speech recognition, call-center deployments have the potential for being a huge market. Call centers are under increasing pressure to automate as a way of reducing cost, attenuating the impact (and cost) of agent turnover, and providing services 24/7. Usually speaker authentication is partnered with speech recognition for customer-facing and partner-facing applications. Most often, speaker authentication is added to existing speech-recognition applications but it is an increasingly popular feature of new deployments as well.

Some call-center applications extend the definition of *speaker authentication*. For most applications, *speaker authentication* is synonymous with *speaker verification*: a one-to-one comparison of the voiceprint of the caller with the system's stored voiceprint for the identity the caller is claiming to have. In the call-center arena there are many applications where more than one person is authorized to access information or engage in secured activities (e.g., joint accounts). When those people share a password, which may occur when the password is an account number, the system needs to compare the caller's voiceprint with stored voiceprints for all of the authorized individuals. When the system only needs to determine whether the speaker belongs to the group of authorized speakers the process is called speaker classification. When the identity of the group member needs to be determined the process is called speaker identification. In either case it entails one-to-many matching.

A voice biometric is a numerical model of the sound, pattern and rhythm of an individual's voice. A voice biometric is as unique to an individual as a finger or palm print. The voice print is established in a registration session or over a period of time as the user continually uses the device.

FIGURE 16A discloses a simplified block diagram for using either the mobile communication device headset of FIGURE 1A or 1B with a personal terminal-based security system. The system can be used for physical access to home or office, as a garage door opener, a car door opener, as a universal handheld remote, for mobile communication device, Internet, and email access and purchases, in addition to making phone calls.

FIGURE 16B discloses a simplified block diagram for using either the mobile communication device of FIGURE 1A or 1B with a corporate terminal-based security system. The system can be used for physical access to home or office, Internet, and email access, for business expenses, currency conversion, managing a stock portfolio, and for making purchases, in addition to making phone calls.

FIGURE 16C discloses a simplified block diagram for using either the mobile communication device of FIGURE 1A or 1B with a resort or luxury cruise terminal-based security system. The system can be used for assigning guests physical access to rooms and restricted areas, gaming activity, entertainment expenses, and for Internet, and email communications, in addition to making phone calls.

FIGURE 16D discloses a simplified block diagram for using either the mobile communication device of FIGURE 1A or 1B with a hospital terminal-based security system. The system can be used for physical access to the hospital and other grounds, for phone, Internet, and email access, and for accessing and updating of patient records.

FIGURE 16E discloses a simplified block diagram for using either the mobile communication device of FIGURE 1A or 1B with a law enforcement terminal-based processing system. The system can be used for headquarters and vehicle access, time and attendance, officer and vehicle tracking, and for phone, Internet, and email communications.

The headset incorporates a microphone configured for capturing audio signals. The headset incorporates processing circuitry, which is configured for analyzing digitized representations of audio signals captured by the microphone. The processing circuitry will include suitable digitization circuitry for providing appropriate representations of the audio signals for further processing. In accordance with another aspect of the present invention, the processing circuitry includes speech detection circuitry, which is configured to analyze the sampled representations of the audio signals to detect speech of the user. The processing circuitry includes circuitry, or interfaces with circuitry, which is configured for transmission of the digitized or sampled representations to a device, such as portable terminal when speech is detected (see for example U.S. Publication No. 20050070337 (Byford et al.) which discloses a wireless headset for use in a speech recognition environment.)

Short-distance wireless communication technologies are used to transmit data from a sensor to a headset, from a headset to a cellphone, from a headset to computer, or from an identification device to a computer. The wireless communicating based on these communication technologies can establish the cordless communication between devices and terminals, thereby simplifying the device connection work and, at the same time, enhancing convenience because it is substantially unnecessary to select installation spaces of the cordlessly connected devices.

The short-distance wireless communication may be used, for example, not only for the data transfer between a computer main frame and its peripheral devices, but also for the data exchange between mobile information devices, and data and audio transmission between a telephone main body, a mobile music player, and a headset, and between a main phone and its cordless headset. Bluetooth™ is the short-distance wireless communication of choice. However, it is to be expressly understood that the metes and bounds of this invention are not to be so limited and that other short-distance wireless communication technologies which include DPOF (Digital Print Order Format) XML (extensible Markup Language), a wireless LAN standardized by IEEE802.11a/b/g/h or the like, UWB (Ultra Wide Band), HAVi™, ZigBee™, NFC, infrared communication, can also be used as short-distance wireless communication schemes.

It is evident that many alternatives, modifications, and variations of the mobile computer terminal of the present invention will be apparent to those skilled in the art in light of the disclosure herein. Thus, a number of preferred embodiments have been fully described above with reference to the drawing figures. The scope of the claims should not be limited by the preferred embodiments and examples, but should be given the broadest interpretation consistent with the description as a whole.

CLAIMS

1. A mobile communication device to be used in a vehicle by a rider in said vehicle, said mobile communication device comprising:

a processor serving as a gatekeeper to access areas secure to an issuing authority, said processor being in short-distance wireless communication to a cell phone;

a headset enabling a digital connection to said issuing authority; and

a fingerprint sensor for capturing fingerprint data, said fingerprint sensor being disposed in said headset;

said headset including:

a speech-transmitting device for transmission of rider speech commands through said short-distance wireless communication, said rider speech commands being submissible to said issuing authority through said short-distance wireless communication to determine rider authorization for rider access; and

an audio device that receives a signal from said short-distance wireless communication, said audio device, in use, being disposed in said headset proximate to one or both ears of said rider;

whereby said headset in combination with said fingerprint sensor provide said rider with phone-centric physical access to a physical area secure to said issuing authority, said issuing authority being someone other than said rider.

2. The mobile communication device of Claim 1, wherein said headset provides said rider with eye-free operation at all times, enabling said rider to focus on driving said vehicle, and said headset provides said rider with hands-free communication at all times other than a finger touch or sweep of said fingerprint sensor to authenticate rider identity.

3. A mobile communication device to be used in a vehicle by a rider in said vehicle, said mobile communication device comprising:

a processor serving as a gatekeeper to access areas secure to an issuing authority, said processor being in short-distance wireless communication to a cell phone;

a headset enabling a digital connection to said issuing authority; and

a fingerprint sensor for capturing fingerprint data, said fingerprint sensor being disposed in said headset;

said headset including:

a speech-transmitting device for transmission of rider speech commands through said short-distance wireless communication, said rider speech commands being submissible to said issuing authority through said short-distance wireless communication to determine rider authorization for rider access; and

an audio device that receives a signal from said short-distance wireless communication, said audio device, in use, being disposed in said mobile communication device proximate to one or both ears of said rider;

whereby said speech-transmitting device in combination with said fingerprint sensor provide said rider with phone-centric financial access to funds secure to said issuing authority, said issuing authority being someone other than said rider; and

whereby a databank external to said mobile communication device compares said sensed fingerprint data with reference fingerprint data if said issuing authority has authorized said data access.

4. A mobile communication device to be used in a vehicle by a rider in said vehicle, said mobile communication device comprising:

a processor serving as a gatekeeper to access areas secure to an issuing authority, said processor being in short-distance wireless communication to a cell phone;

a headset enabling a digital connection to said issuing authority; and

a fingerprint sensor for capturing fingerprint data, said fingerprint sensor being disposed in said headset;

said headset including:

a speech-transmitting device for transmission of rider speech commands through said short-distance wireless communication, said rider speech commands being submissible to said issuing authority through said short-distance wireless communication to determine rider authorization for rider access; and

an audio device that receives a signal from said short-distance wireless communication, said audio device, in use, being disposed in said mobile communication device proximate to one or both ears of said rider;

whereby said speech-transmitting device in combination with said fingerprint sensor provide said rider with phone-centric data access to data secure to said issuing authority, said issuing authority being someone other than said rider; and

whereby a databank external to said mobile communication device compares said sensed fingerprint data with reference fingerprint data if said issuing authority has authorized said data access.

5. A mobile communication device to be used in a vehicle by a rider in said vehicle, said mobile communication device comprising:

a processor serving as a gatekeeper to access areas secure to an issuing authority, said processor being in short-distance wireless communication to a cell phone;

a headset enabling a digital connection to said issuing authority; and

a fingerprint sensor for capturing fingerprint data, said fingerprint sensor being disposed in said headset;

said headset including:

a speech-transmitting device for transmission of user speech commands through said short-distance wireless communication, said user speech commands being submissible to said issuing authority through said short-distance wireless communication to determine user authorization for user access; and

an audio device that receives a signal from said short-distance wireless communication, said audio device, in use, being disposed in said headset proximate to one or both ears of said user;

whereby said headset in combination with said fingerprint sensor provide said user with phone-centric physical access for vehicle entry secure to said issuing authority, said issuing authority being someone other than said rider.

6. A method for enabling a user to gain physical access to a secure area via a wearable computer as approved by an issuing authority, said method comprising:

receiving a user request at a processor remote from said wearable computer for physical access into said secure area;

authorizing said wearable computer at a processor remote from said wearable computer if said wearable computer has been authorized for purpose of said user request by said issuing authority;

prompting said wearable computer from a processor remote from said wearable computer that submission of fingerprint data is needed to gain said physical access into said secure area;

receiving said user fingerprint data submitted from said wearable computer of a processor remote from said wearable computer, said wearable computer enabling said user to have both hands free except when submitting said fingerprint data via a fingerprint sensor disposed in said wearable computer, reference fingerprint data having been previously provided for authentication during a registration; and

comparing said user fingerprint data with said reference fingerprint data in a processor remote from said wearable computer, and approving said user request for said physical

access to said secure area if said user is authorized for said access by said issuing authority, said authentication of user identity being made at least in part based upon said comparison of said user fingerprint data and said reference fingerprint data.

7. A method for enabling a user to gain financial access via a wearable computer as approved by an issuing authority, said method comprising:

receiving a user request at a processor remote from said wearable computer for financial access to purchase goods or services at a terminal;

authorizing said wearable computer at a processor remote from said wearable computer if said wearable computer has been authorized for purpose of said user request by said issuing authority;

prompting said wearable computer from a processor remote from said wearable computer that submission of fingerprint data is needed to gain said financial access;

receiving said user fingerprint data submitted from said wearable computer of a processor remote from said wearable computer, said wearable computer enabling said user to have both hands free except when submitting said fingerprint data via a fingerprint sensor disposed in said wearable computer, reference fingerprint data having been previously provided for authentication during a registration; and

comparing said user fingerprint data with said reference fingerprint data in a processor remote from said wearable computer, and approving said user request to gain said financial access if said user is authorized by said issuing authority and an account balance has not been exceeded, said authentication of user identity being made at least in part based upon a comparison of said sensed fingerprint data and reference fingerprint data.

8. A method for enabling a user to gain data access to a secure network via a wearable computer as approved by an issuing authority, said method comprising:

receiving a user request at a processor remote from said wearable computer for access to or entry of secure data in a secure network;

authorizing said wearable computer at a processor remote from said wearable computer if said wearable computer has been authorized for purpose of said user request by said issuing authority;

prompting said wearable computer from a processor remote from said wearable computer that submission of fingerprint data is needed to gain said access to said secure network;

receiving said user fingerprint data submitted from said wearable computer of a processor remote from said wearable computer, said wearable computer enabling said user to have both hands free except when submitting said fingerprint data via a fingerprint sensor disposed in said wearable computer, reference fingerprint data having been previously provided for authentication during a registration; and

comparing said user fingerprint data with said reference fingerprint data in a processor remote from said wearable computer, and approving said user request for said data access to said secure network if said user is authorized, said authentication of user identity being made at least in part based upon a comparison of said sensed fingerprint data and reference fingerprint data.

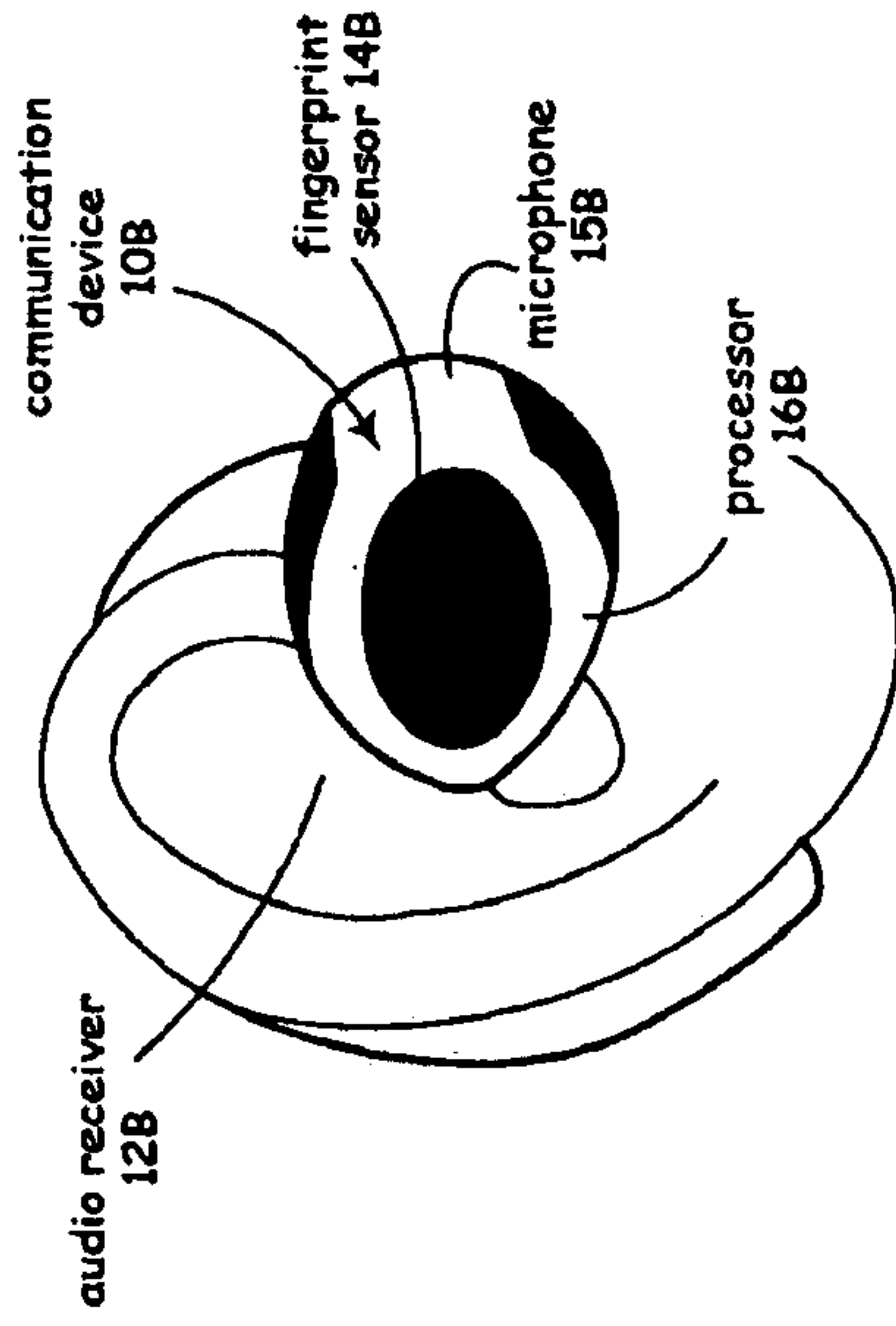
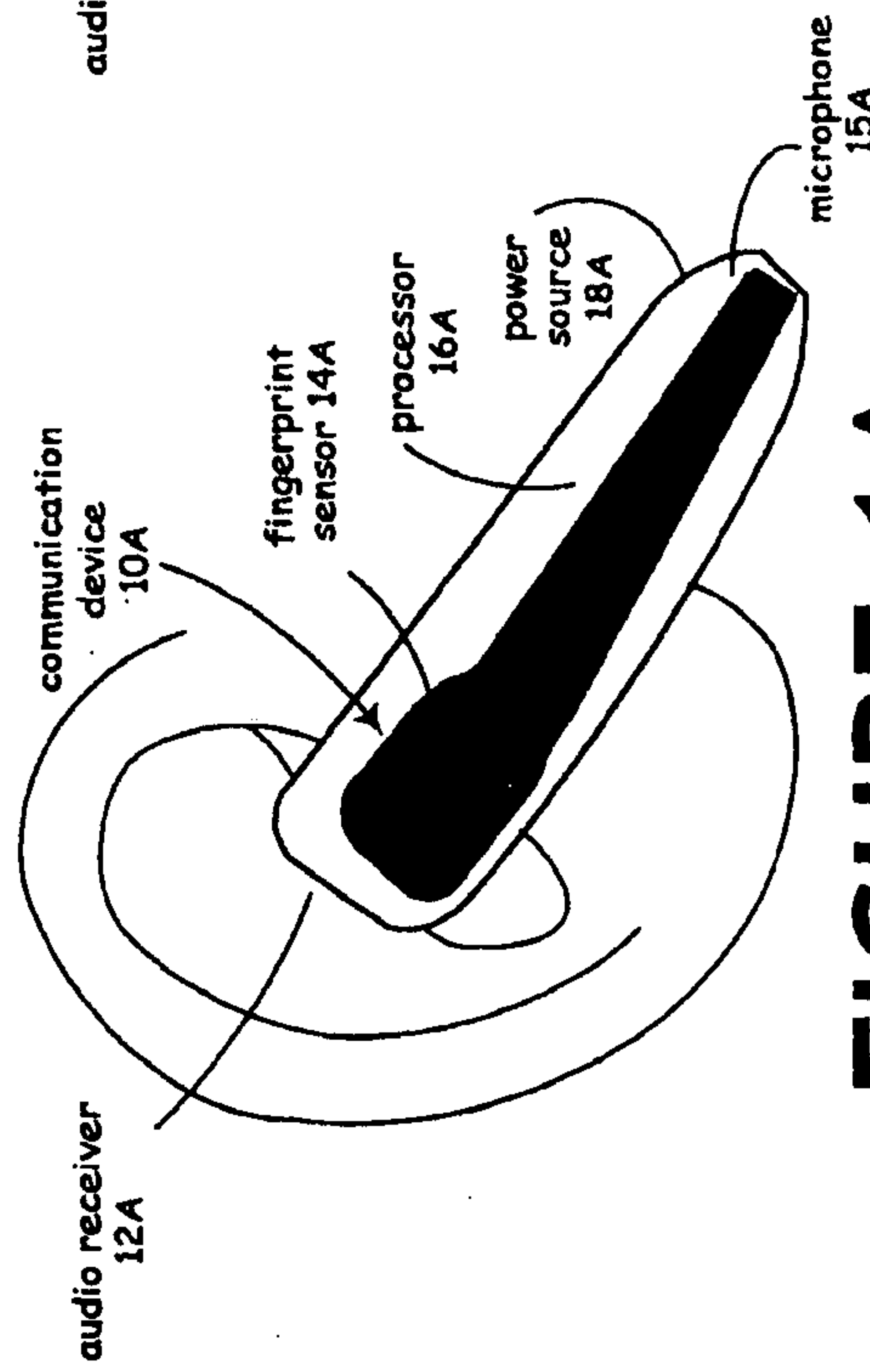


FIGURE 1C

EYE-COVERING COMMUNICATION DEVICE

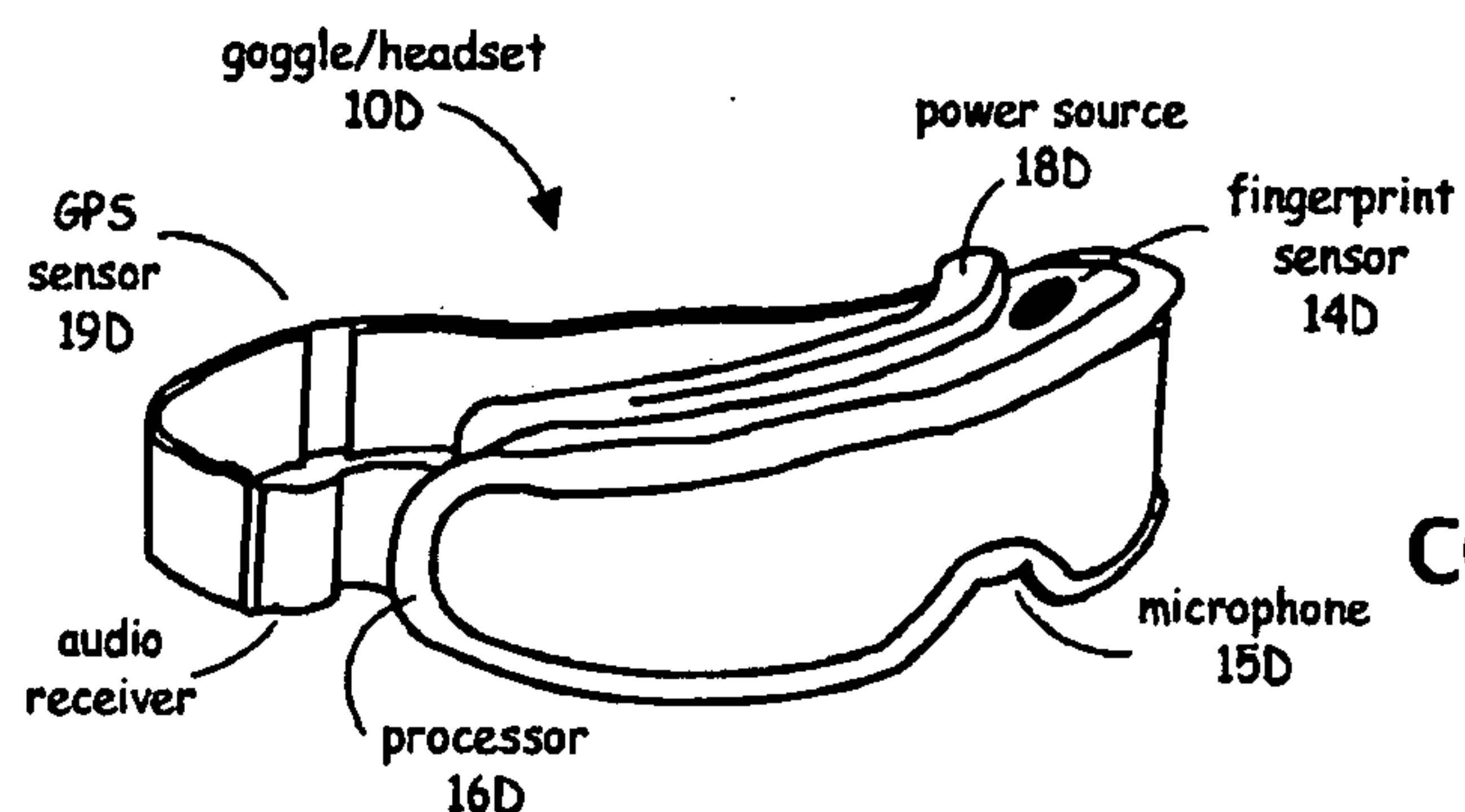
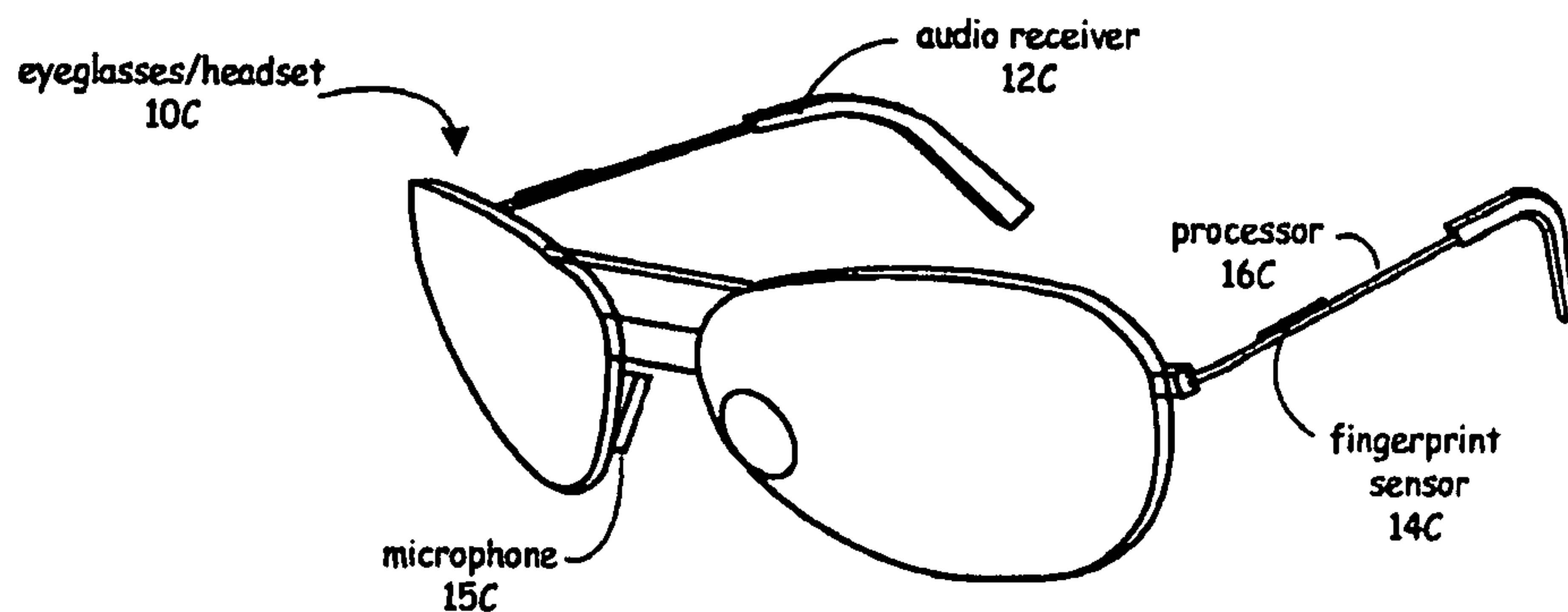


FIGURE 1D

EYE-COVERING COMMUNICATION DEVICE

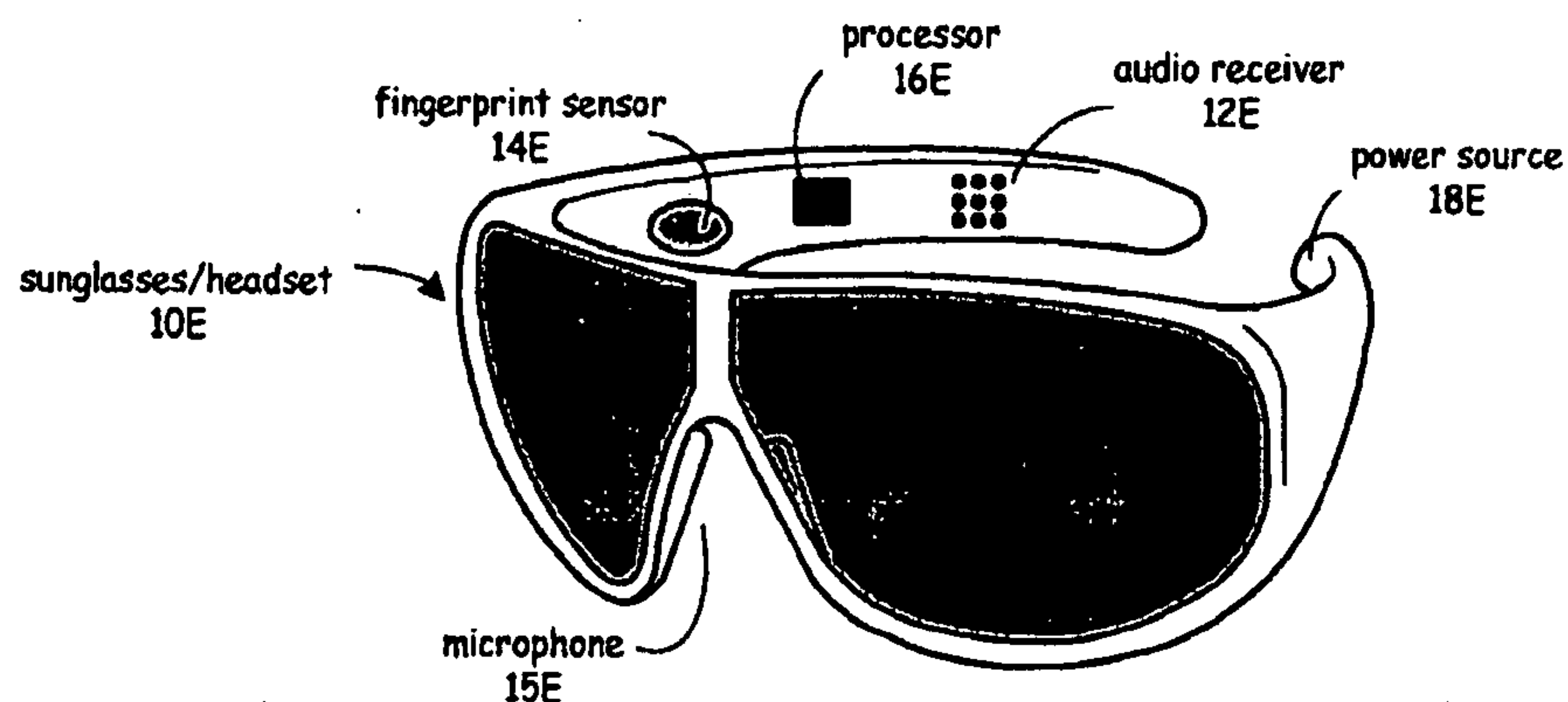


FIGURE 1E

EYE-COVERING COMMUNICATION DEVICE

FIGURE 1F
HEAD-COVERING
COMMUNICATION DEVICE

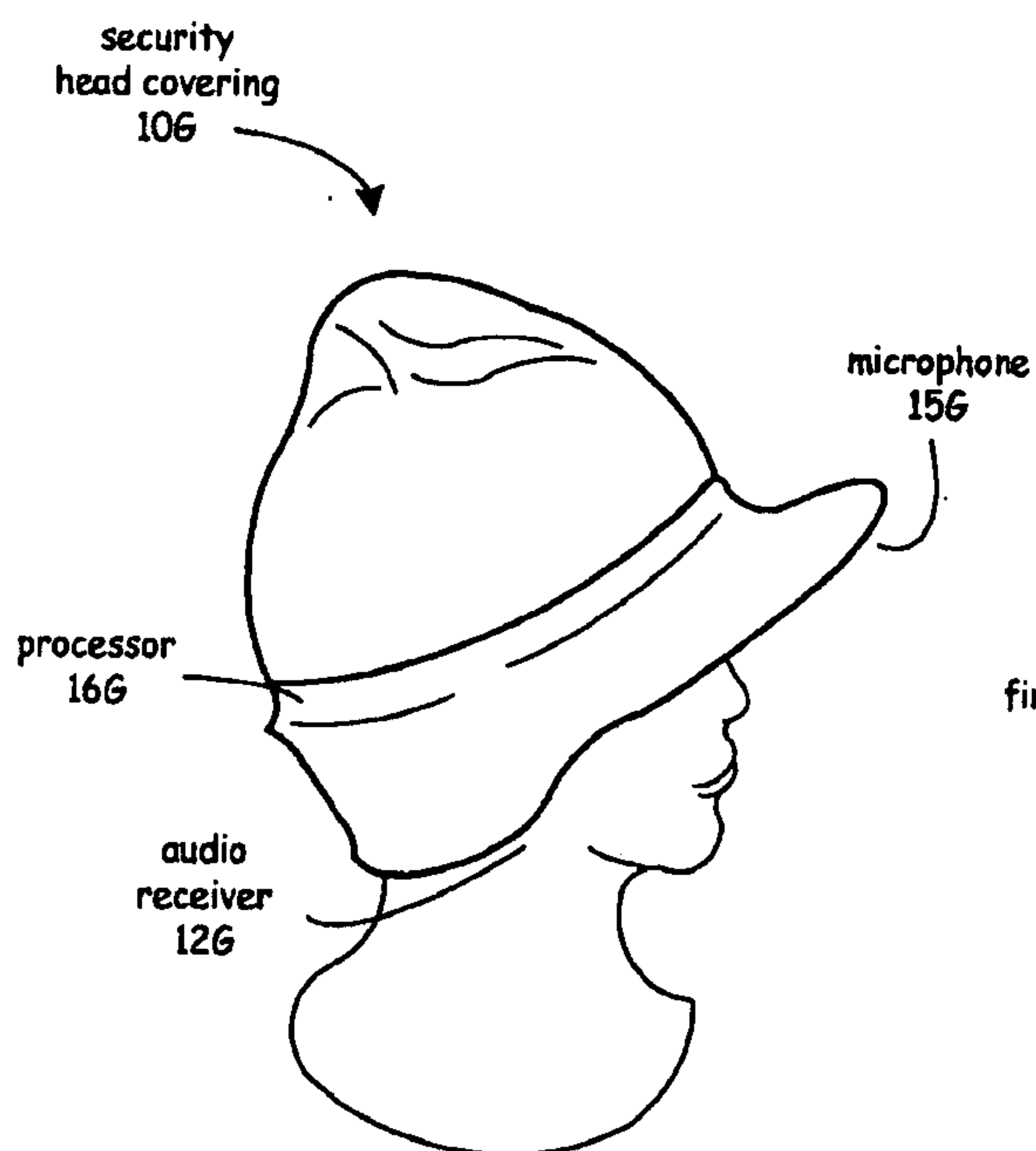
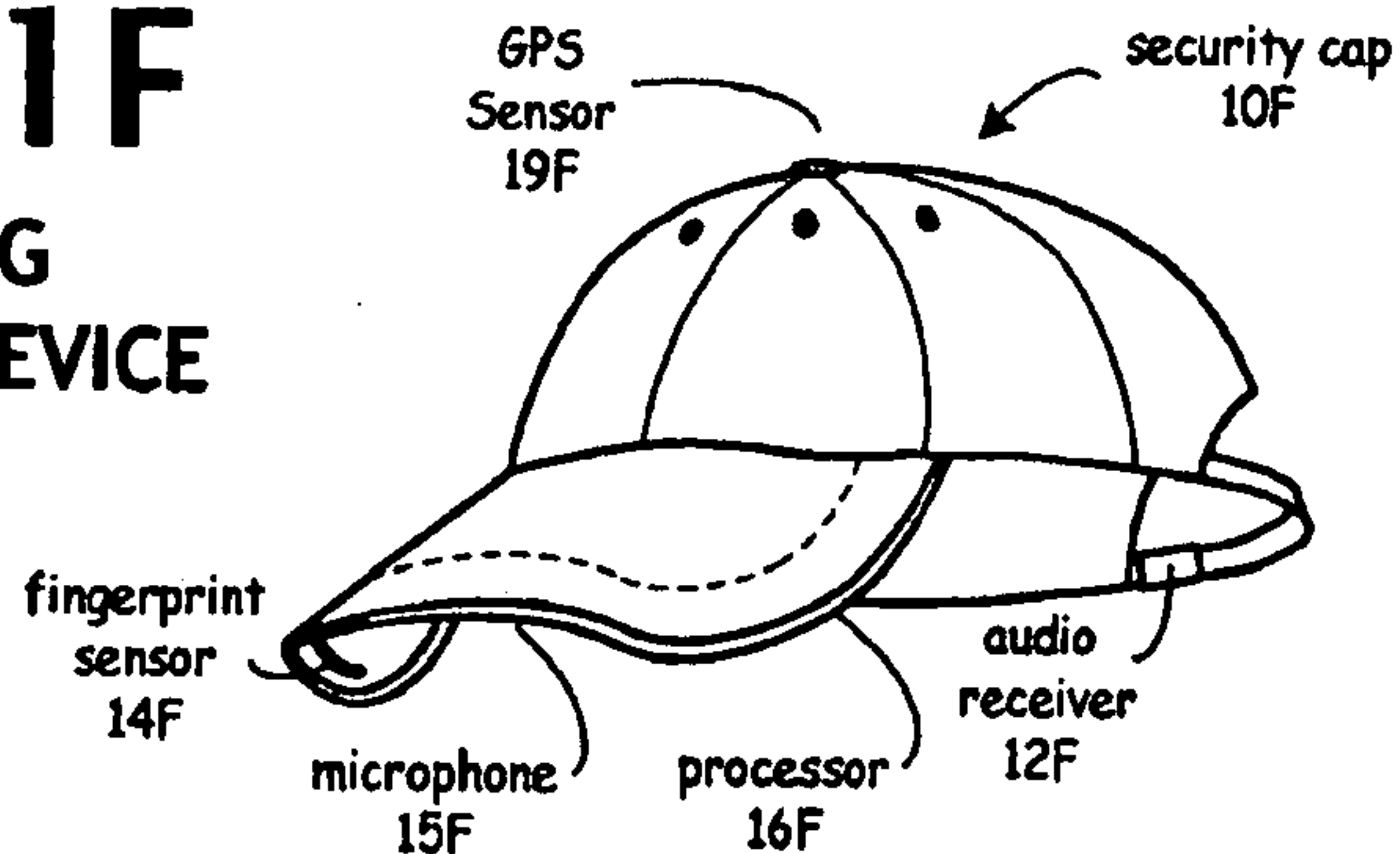


FIGURE 1G
HEAD-COVERING
COMMUNICATION DEVICE

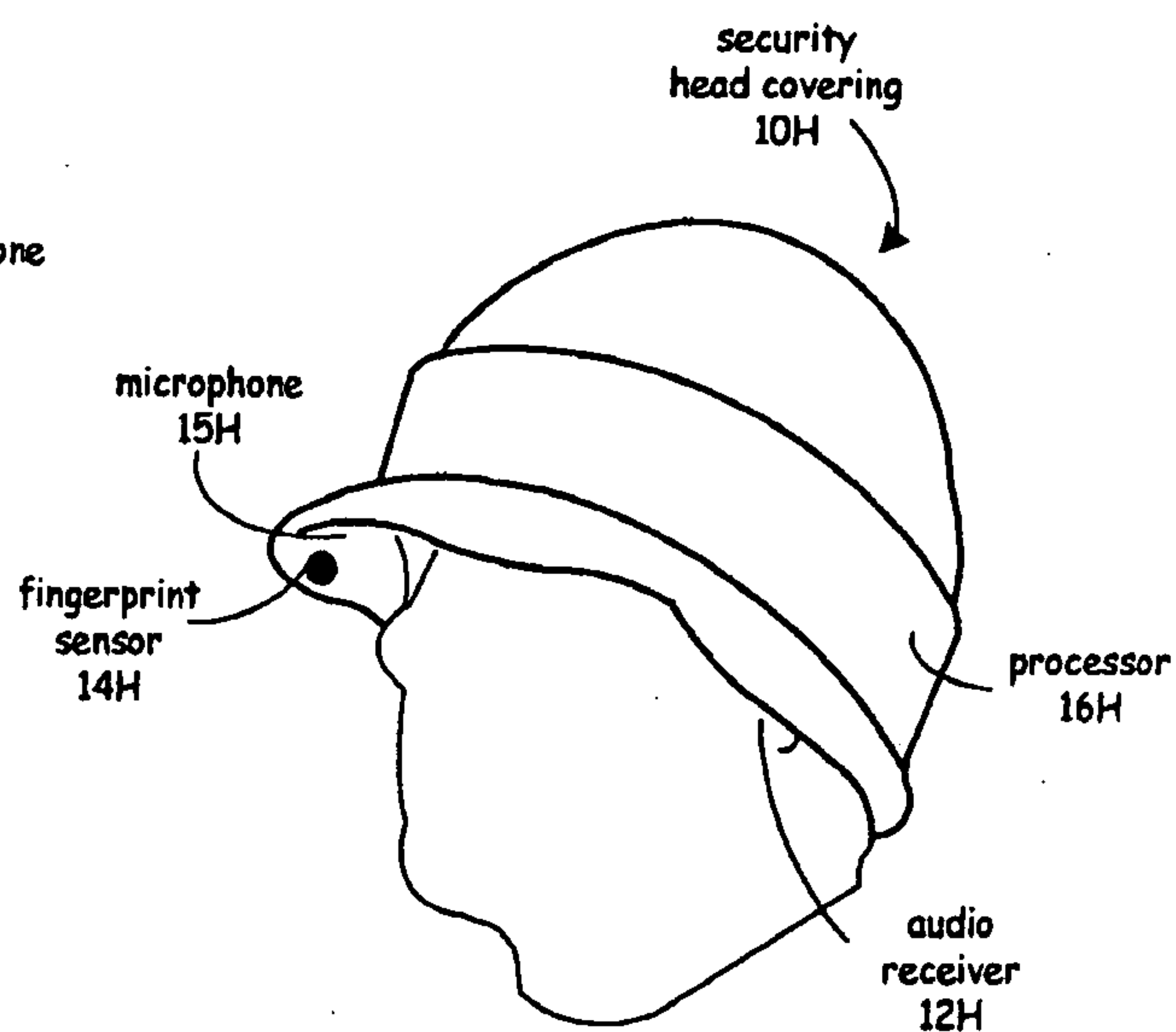


FIGURE 1H
HEAD-COVERING
COMMUNICATION DEVICE

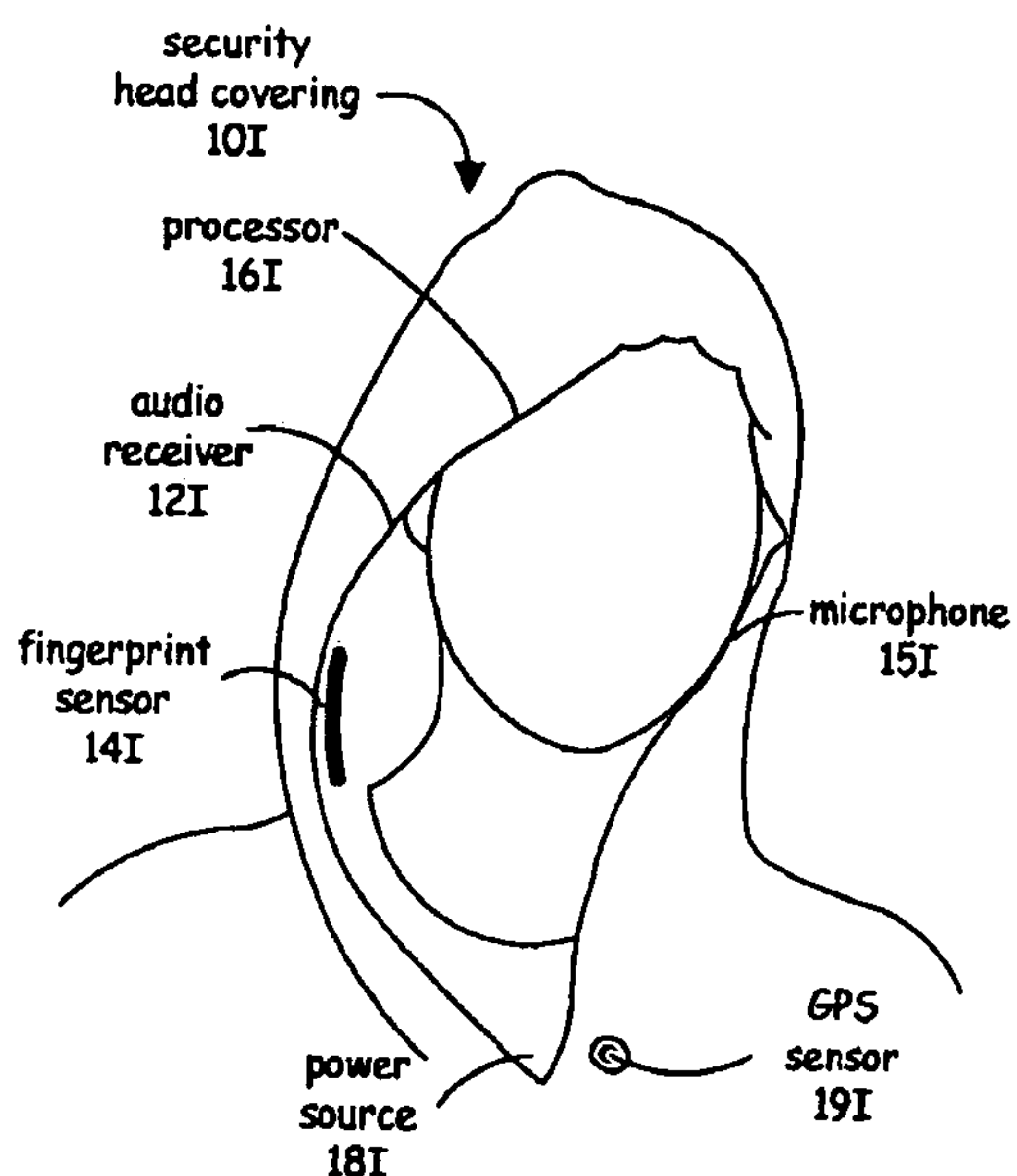


FIGURE 1I
HEAD-COVERING
COMMUNICATION DEVICE

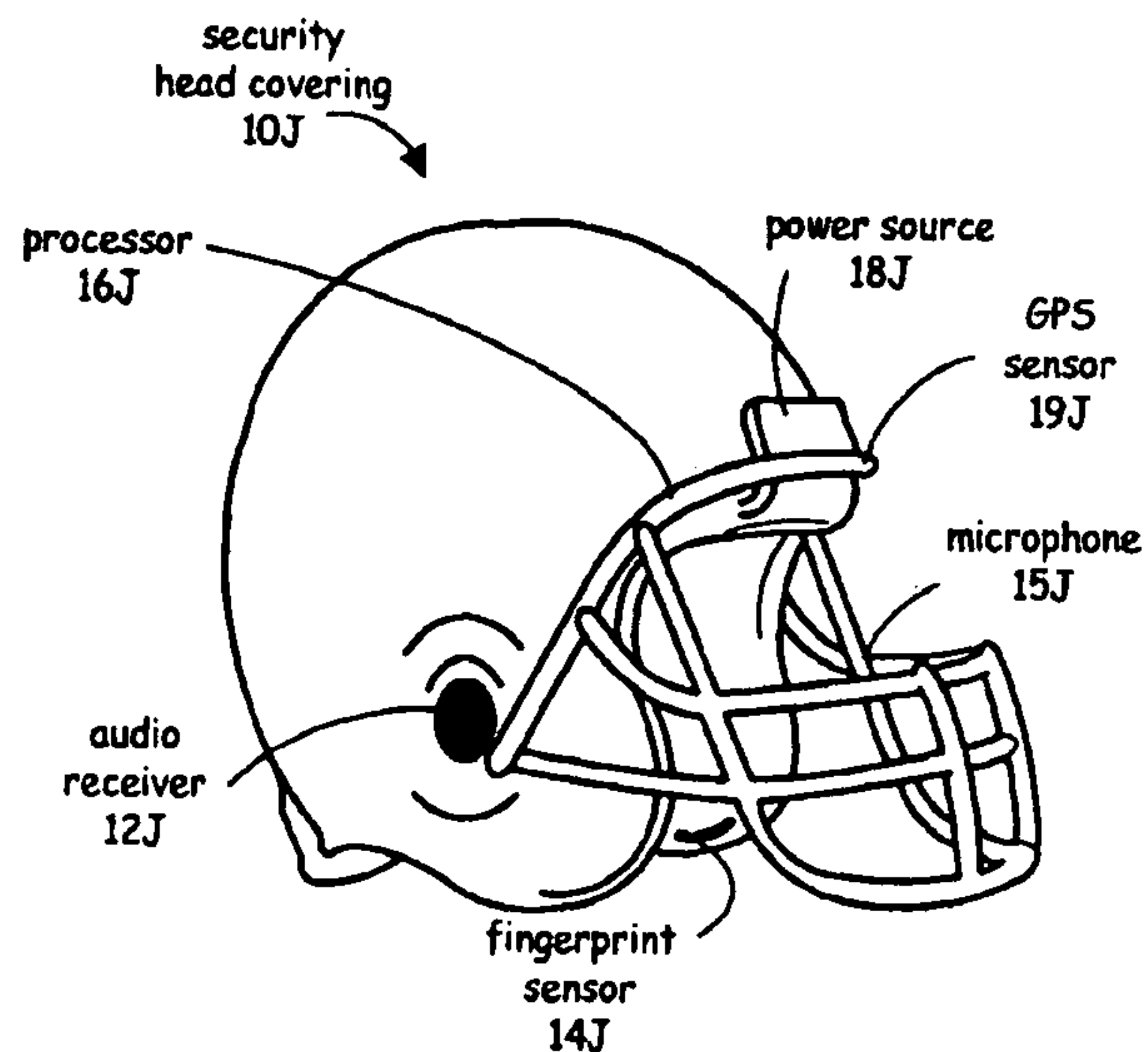


FIGURE 1J
HEAD COVERING
COMMUNICATION DEVICE

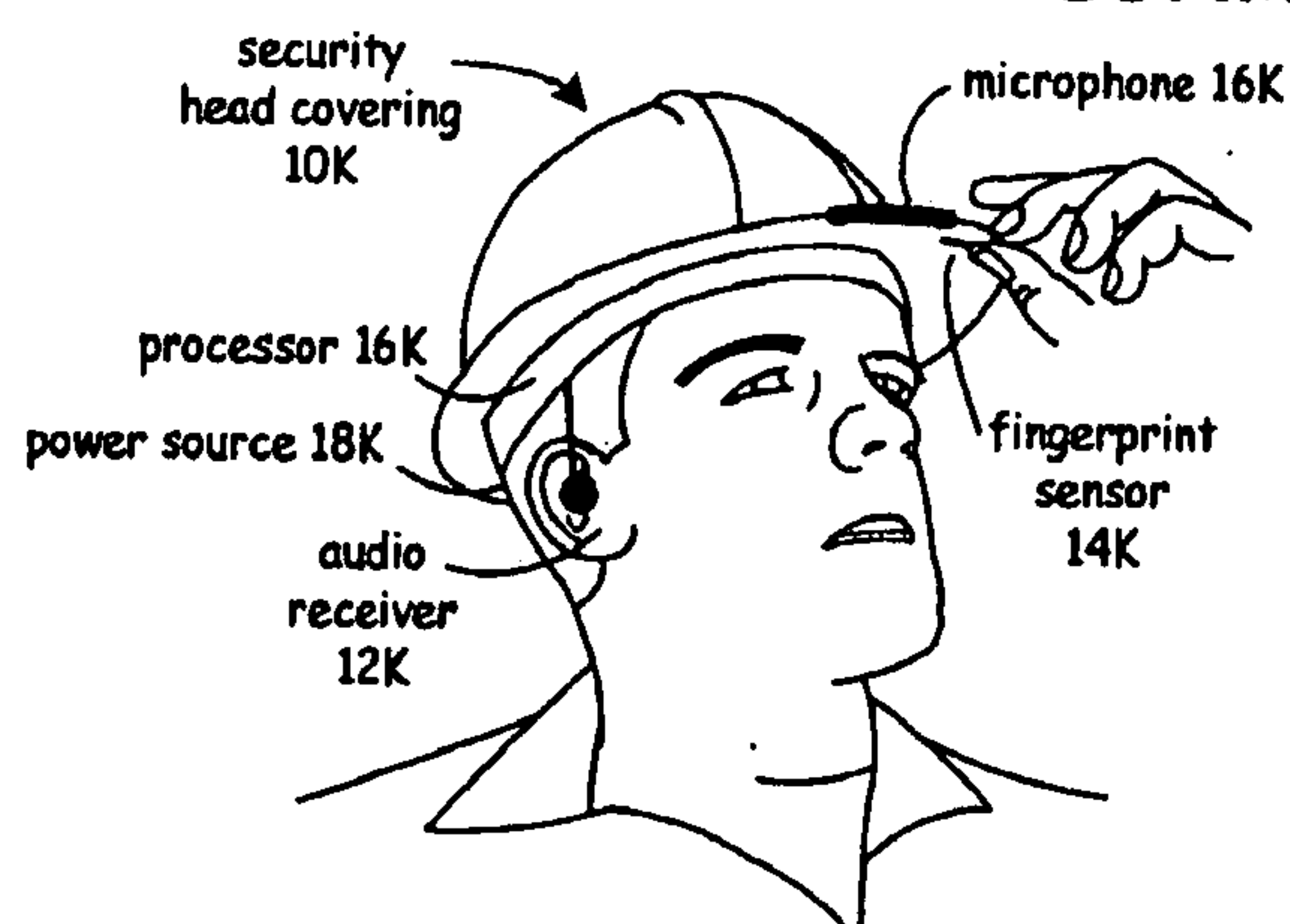


FIGURE 1K
HEAD-COVERING
COMMUNICATION DEVICE

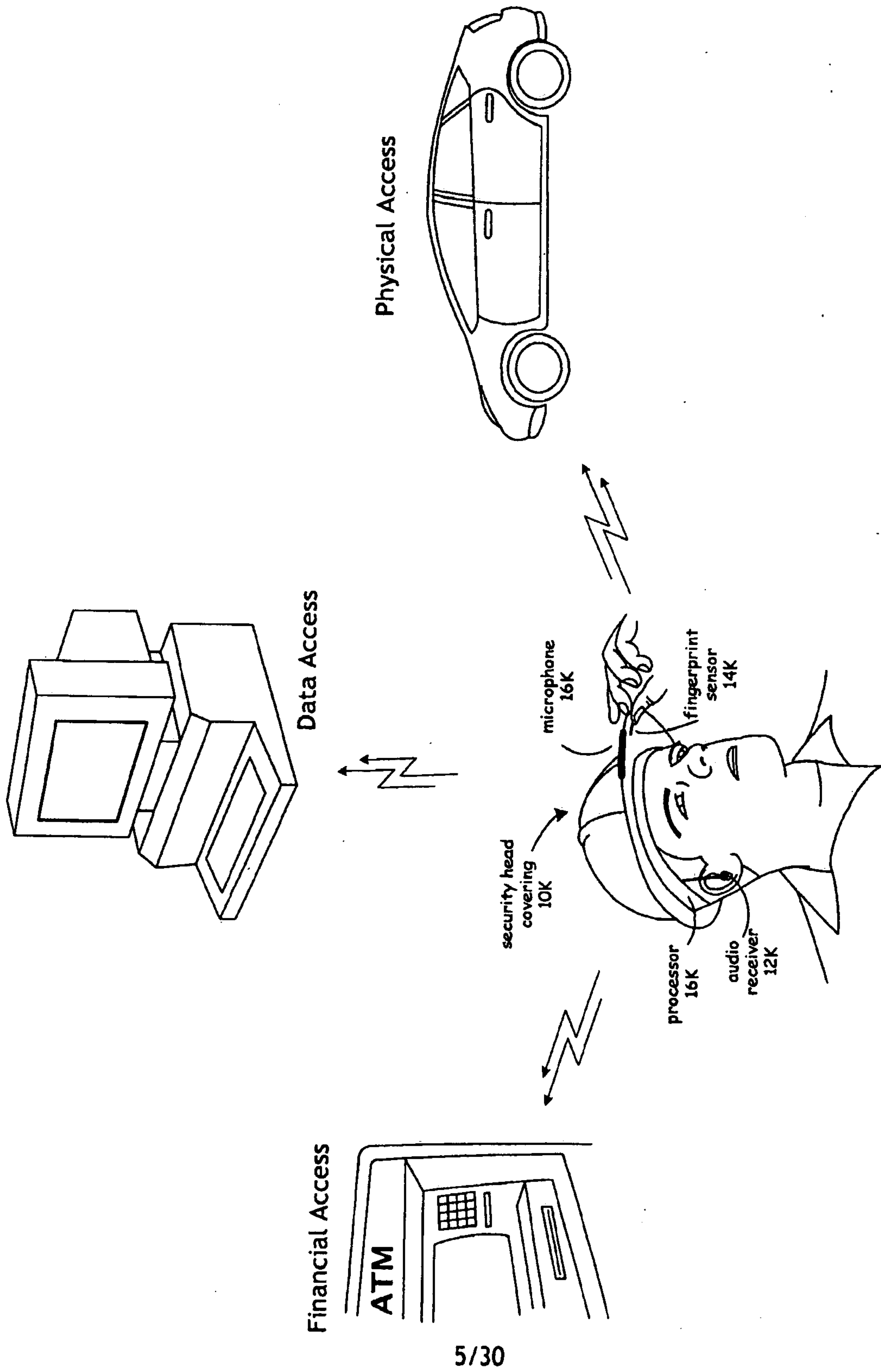
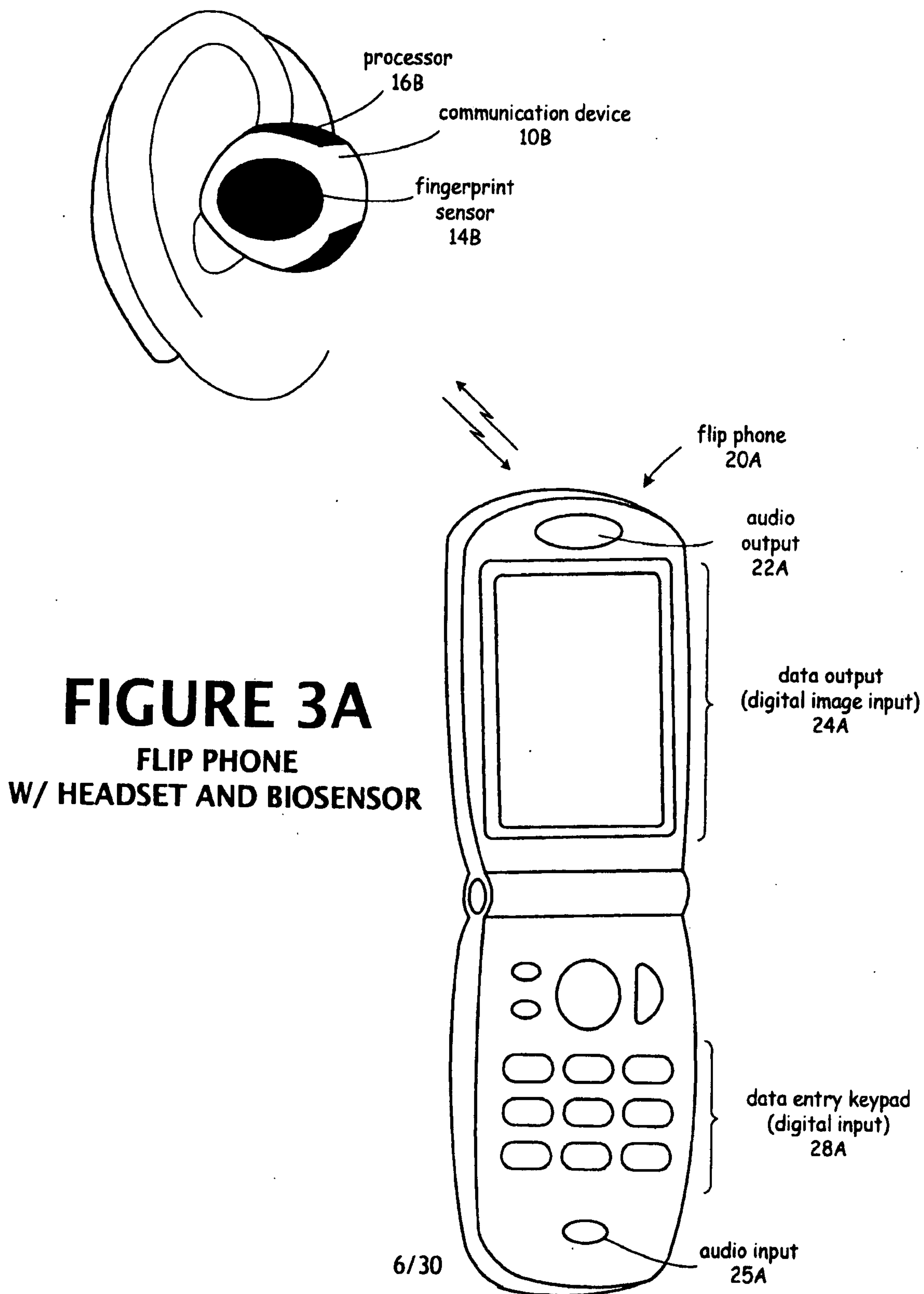


FIGURE 2
FINGERPRINT SECURITY THROUGH A
HEADSET IN A HEAD COVERING



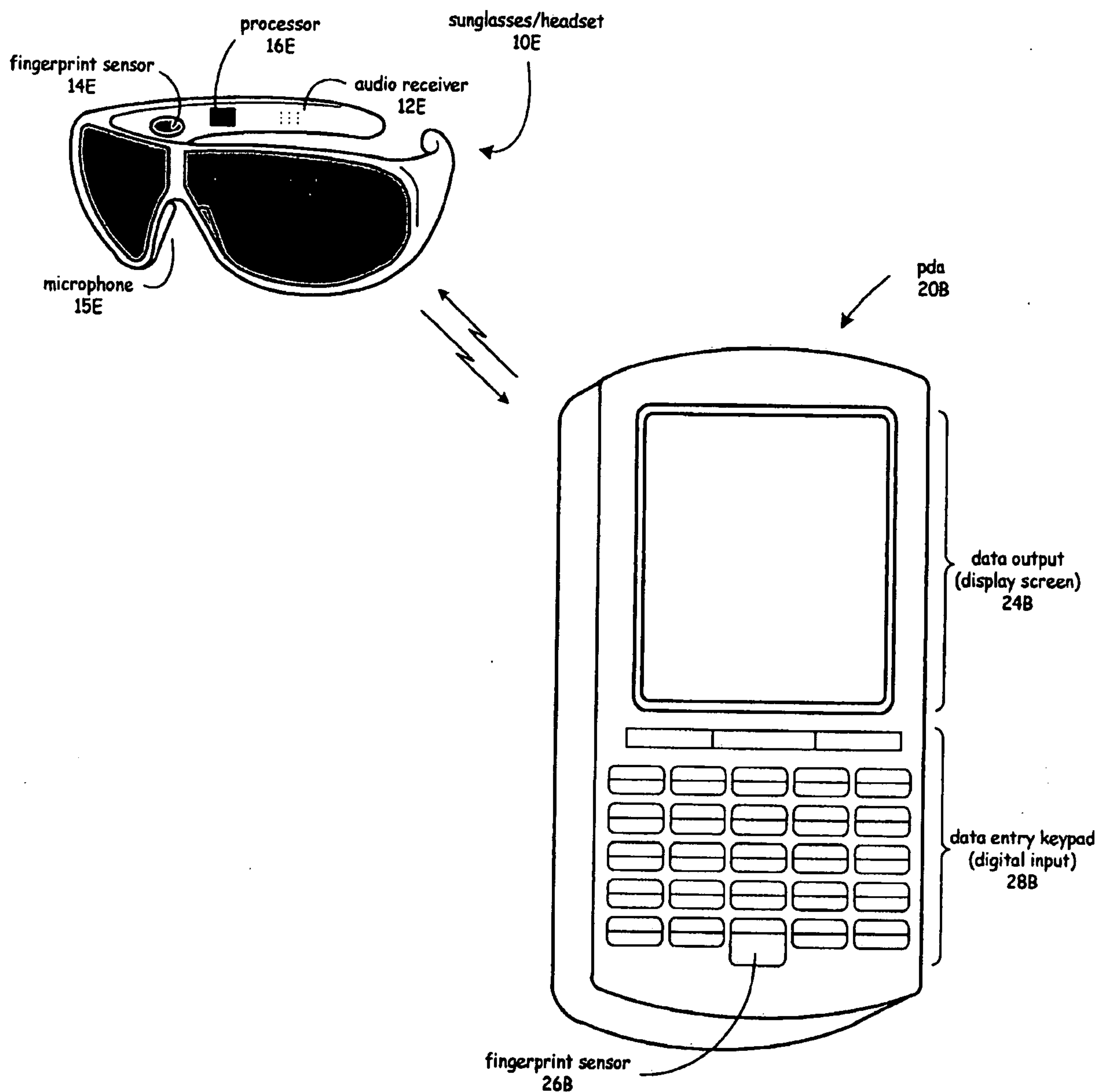


FIGURE 3B
HANDHELD COMPUTER TERMINAL
W/ BLUETOOTH HEADSET
EYEGLASSES

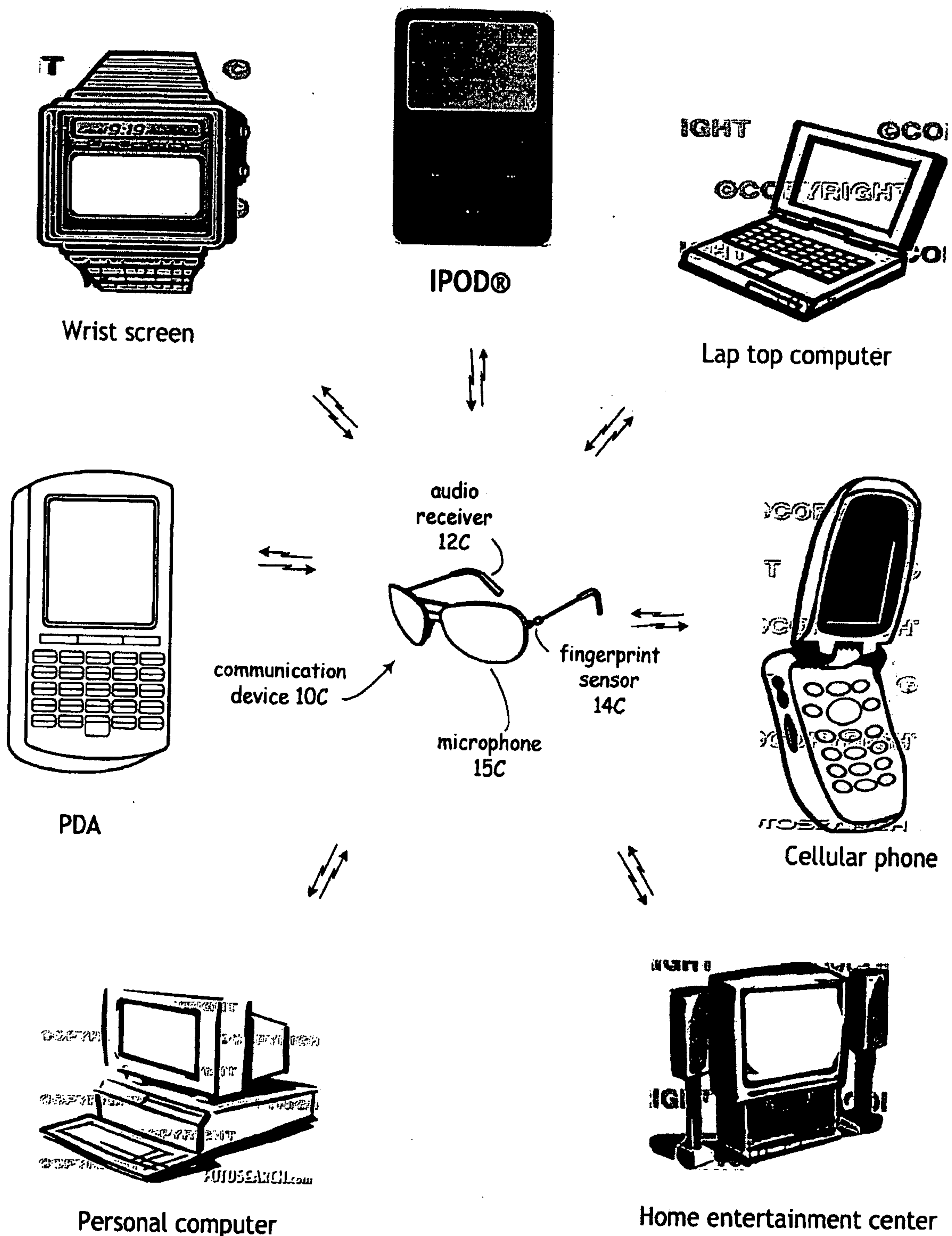
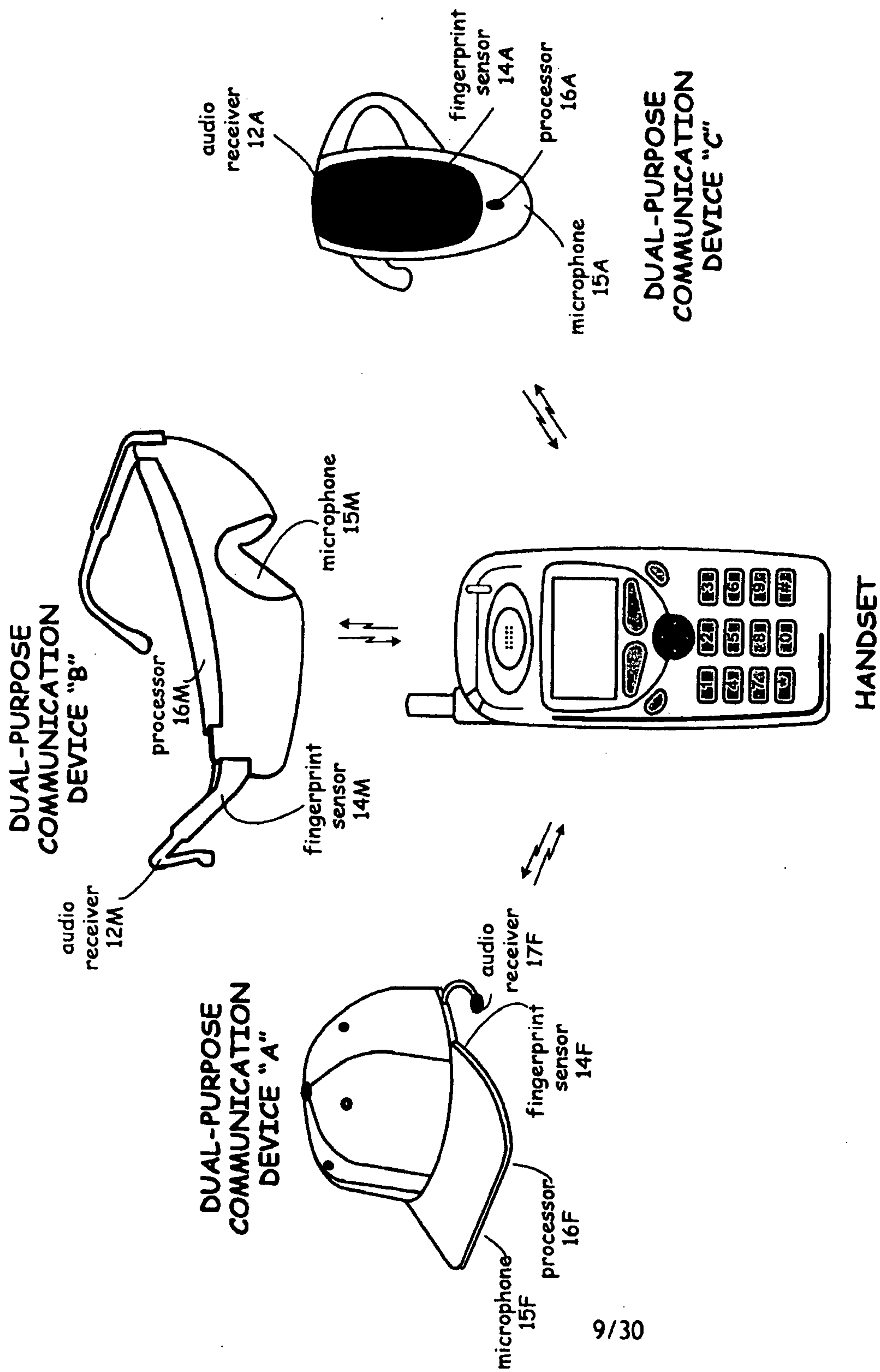


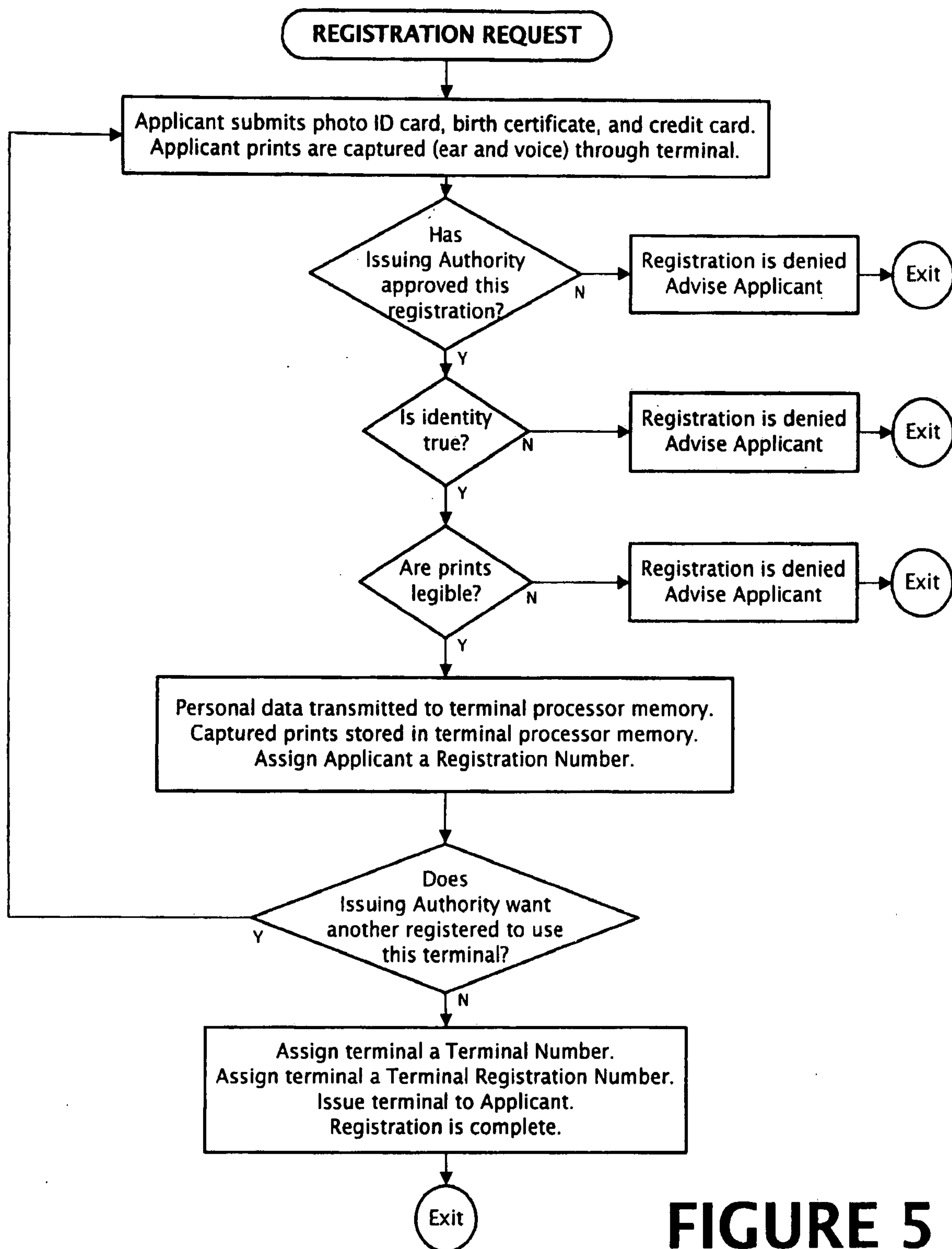
FIGURE 4A

**EYE-COVERING COMMUNICATION DEVICE HAVING
SHORT-DISTANCE WIRELESS COMPATIBILITY
W/ PLURALITY OF COMMUNICATION DEVICES**

8/30

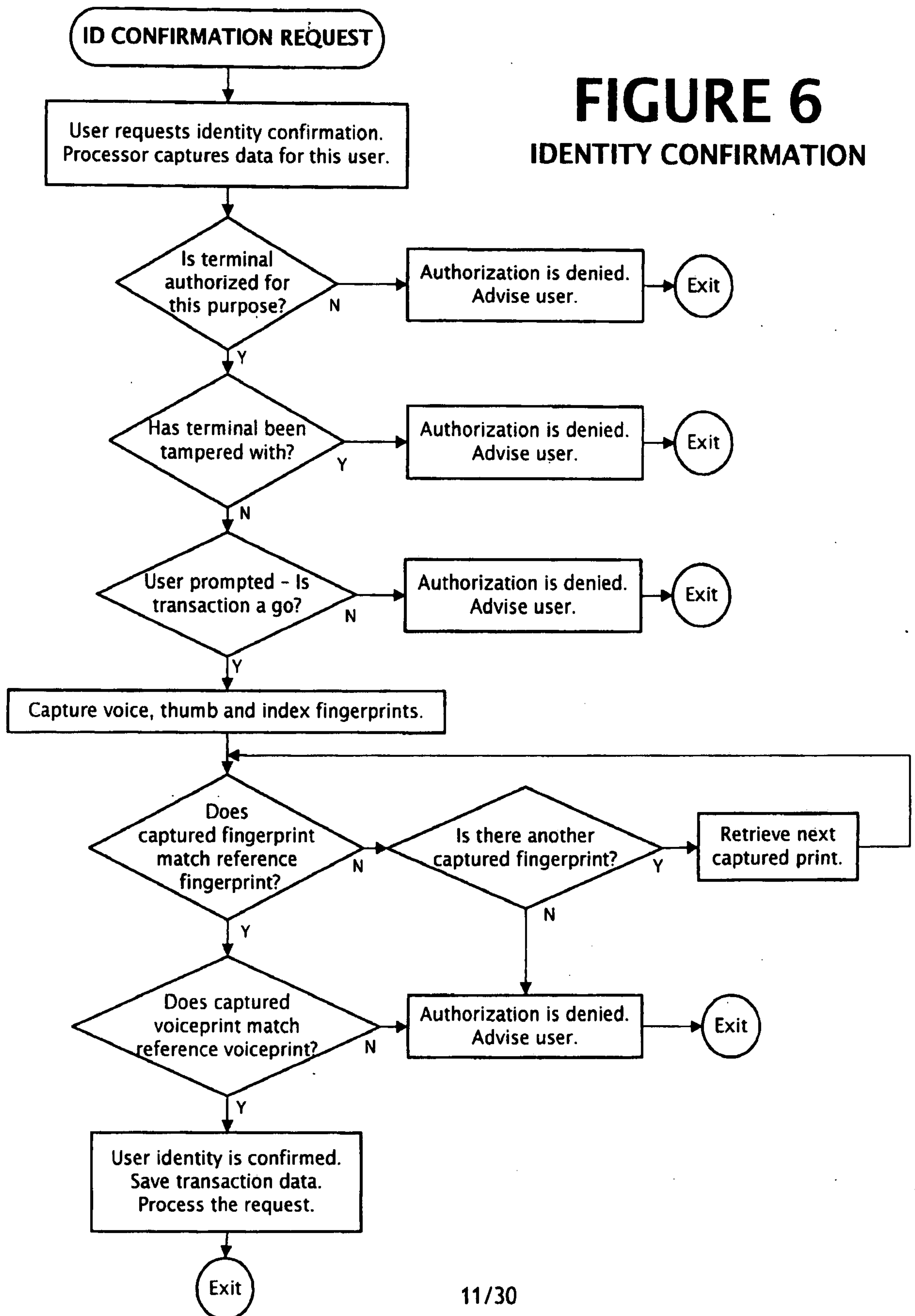
**FIGURE 4B**

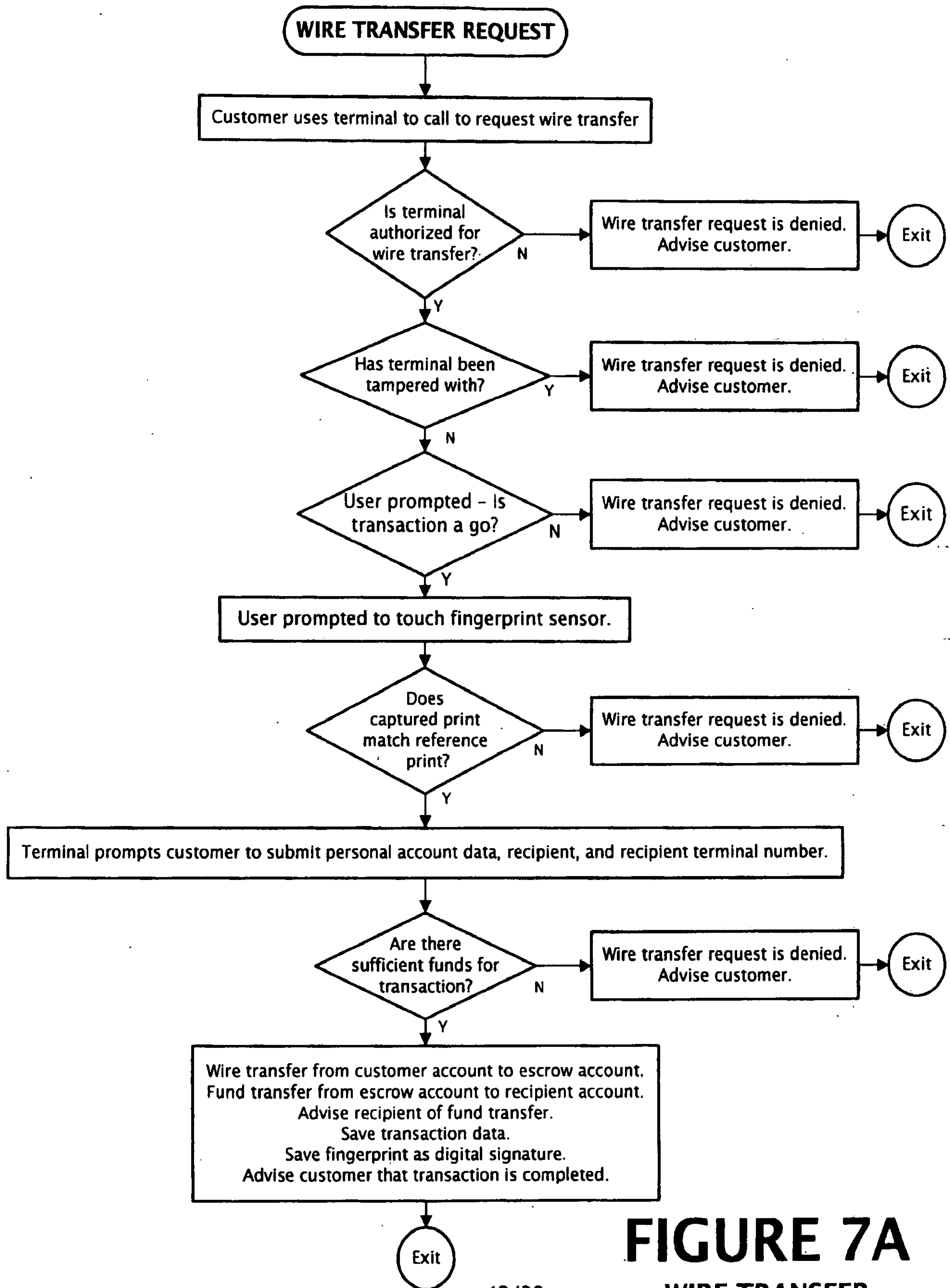
HANDSET COMPATIBLE W/ PLURALITY OF DUAL-PURPOSE COMMUNICATION DEVICES



10/30

FIGURE 5
TERMINAL REGISTRATION





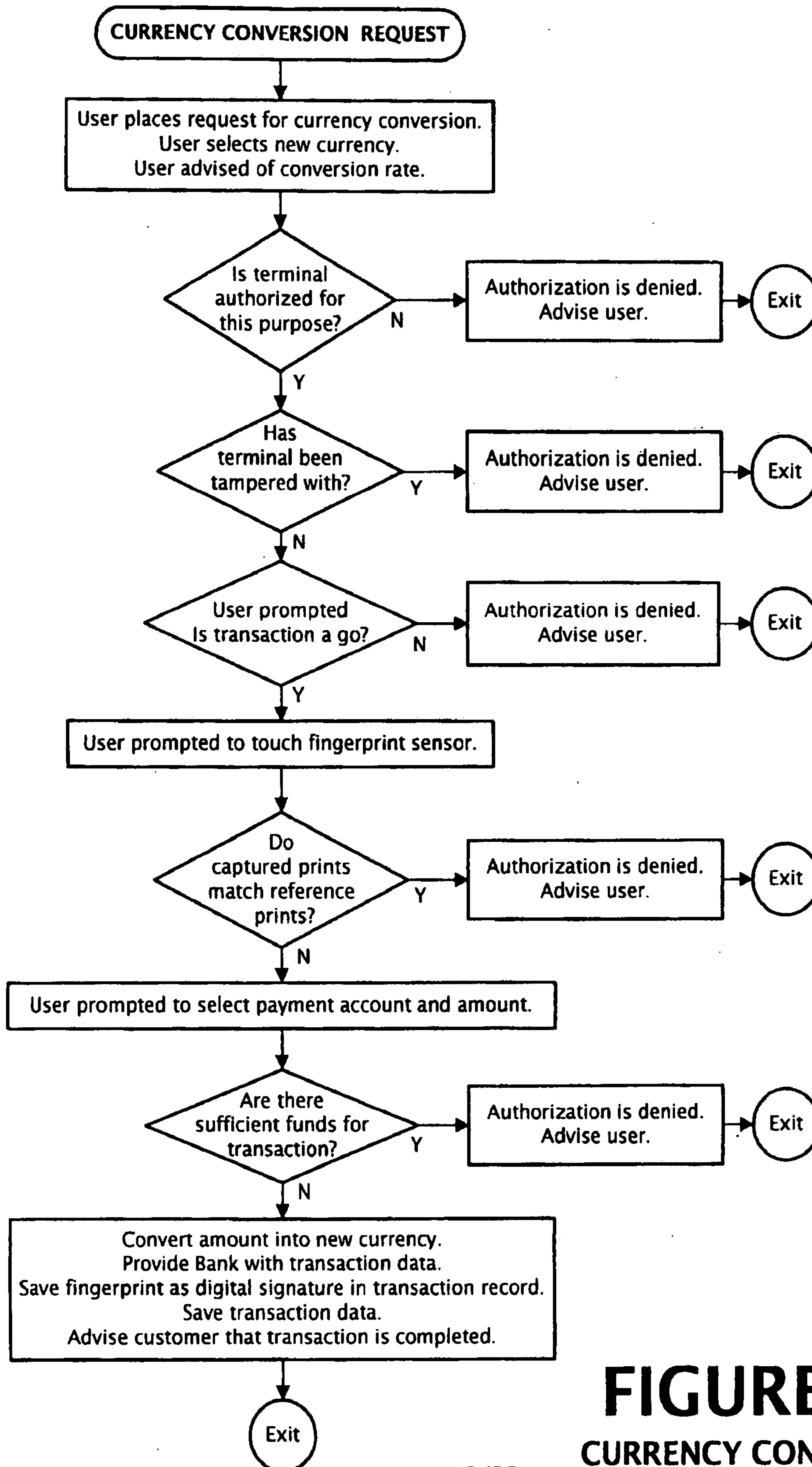


FIGURE 7B
CURRENCY CONVERSION

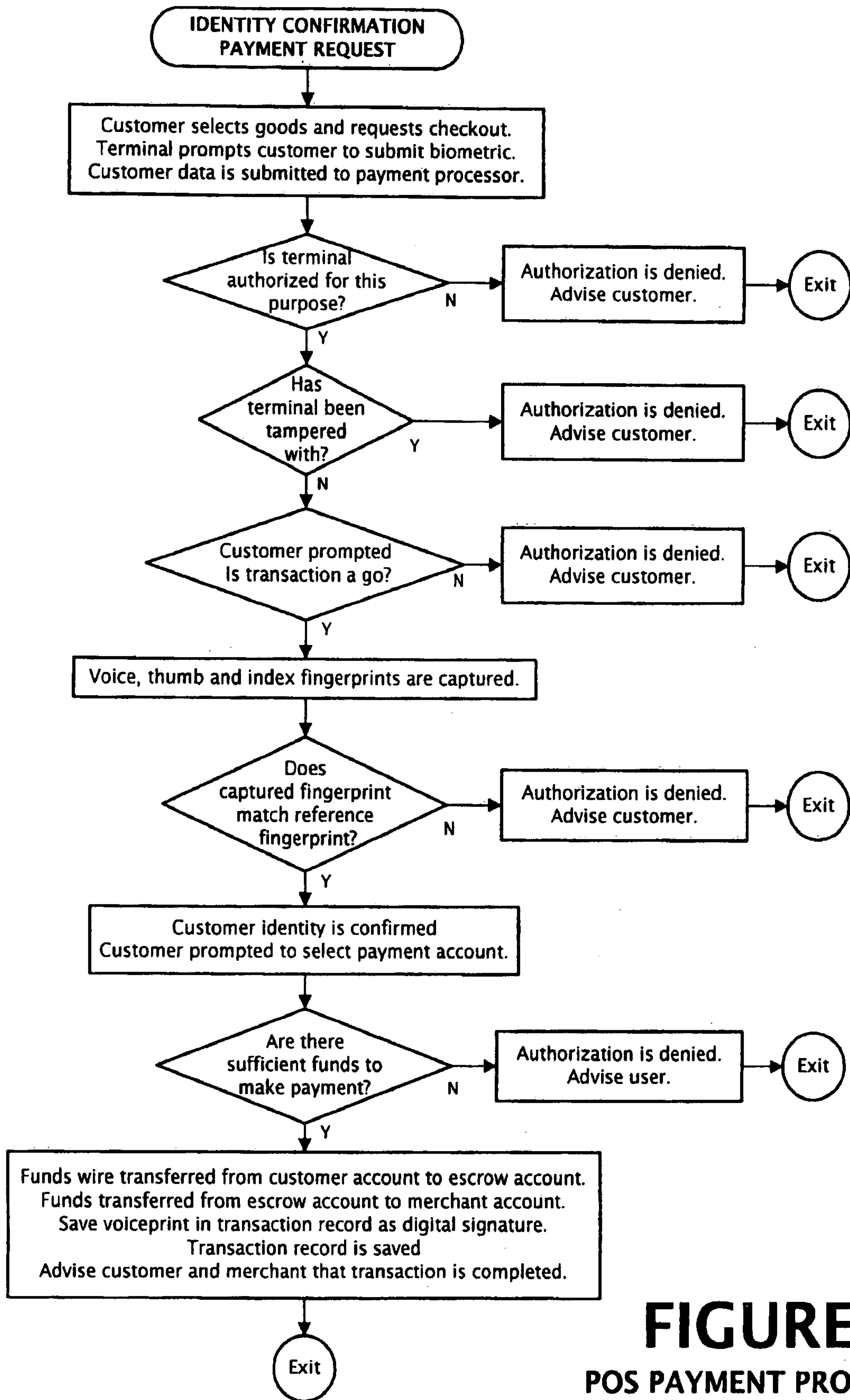
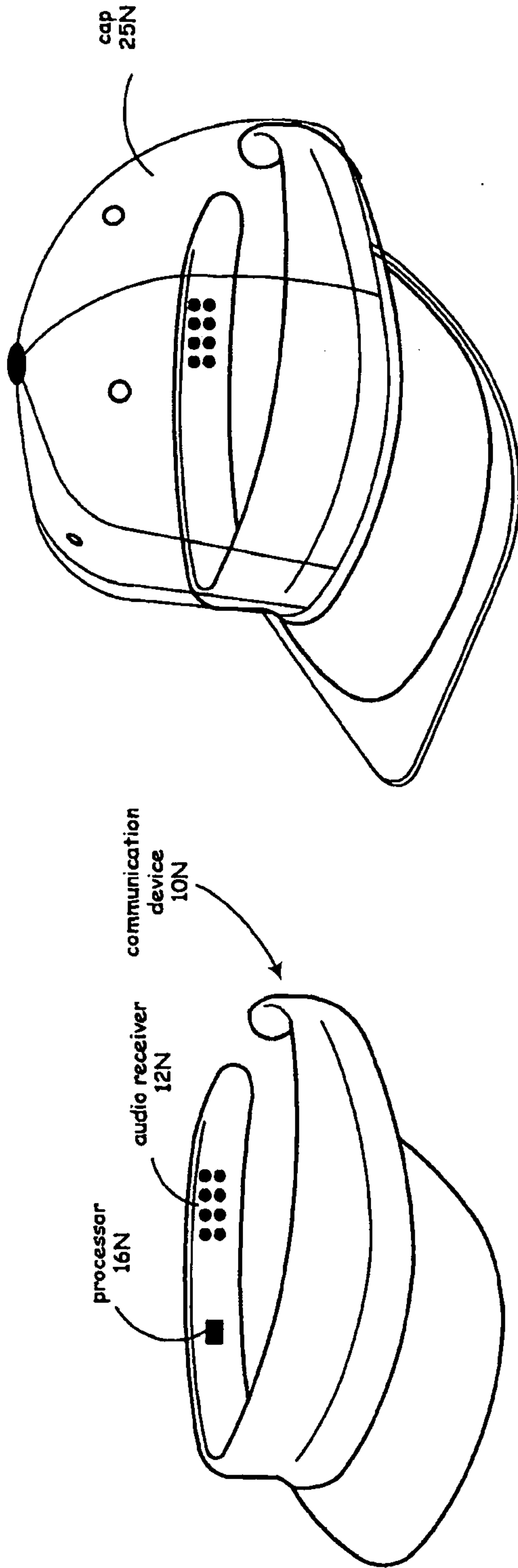


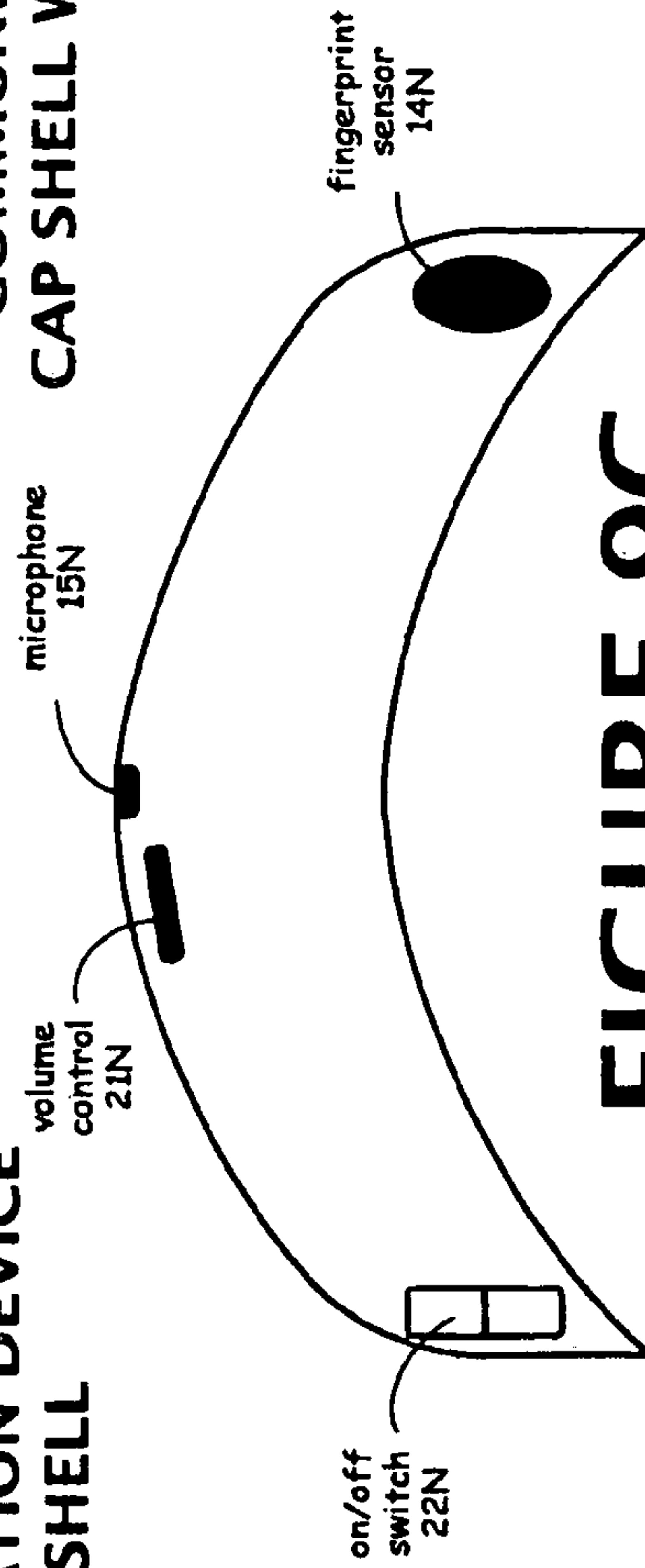
FIGURE 8
POS PAYMENT PROCESSING

**FIGURE 9A**

COMMUNICATION DEVICE
CAP SHELL

FIGURE 9B

COMMUNICATION DEVICE
CAP SHELL W/ CONVENTIONAL
CAP

**FIGURE 9C**

UNDERSIDE OF CAP SHELL

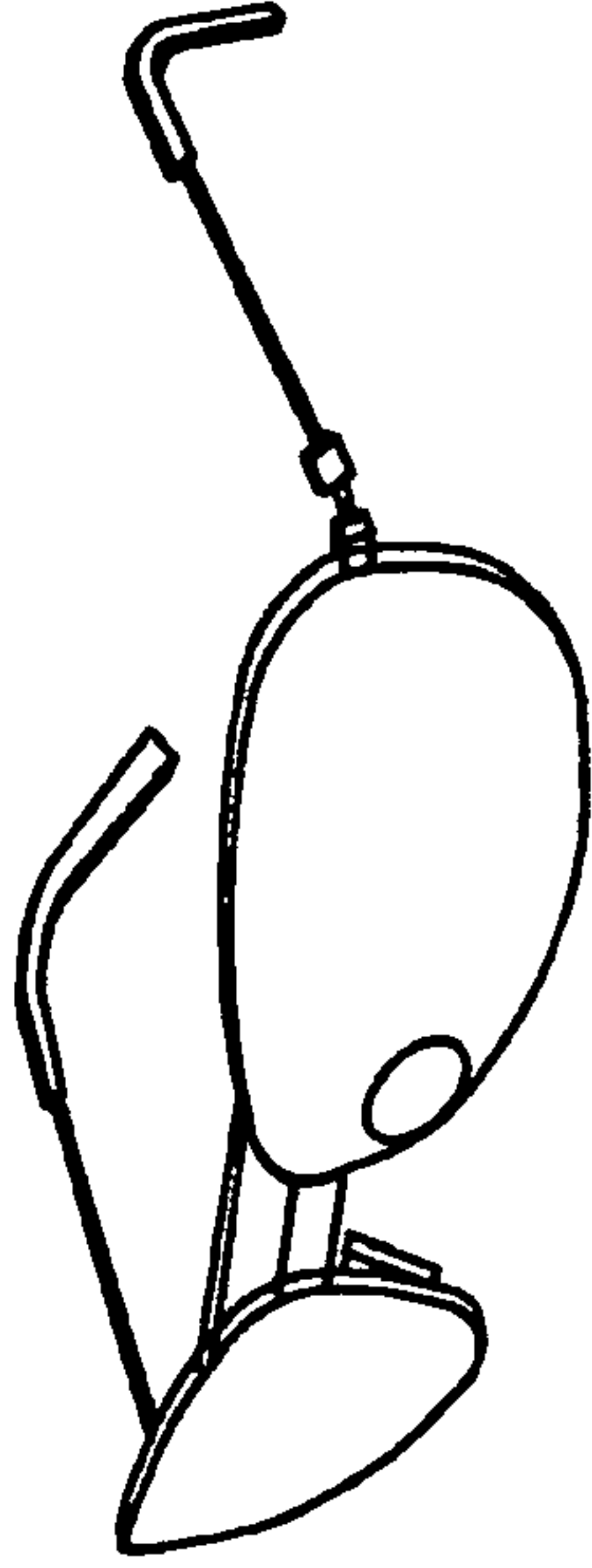


FIGURE 10A
GLASSES

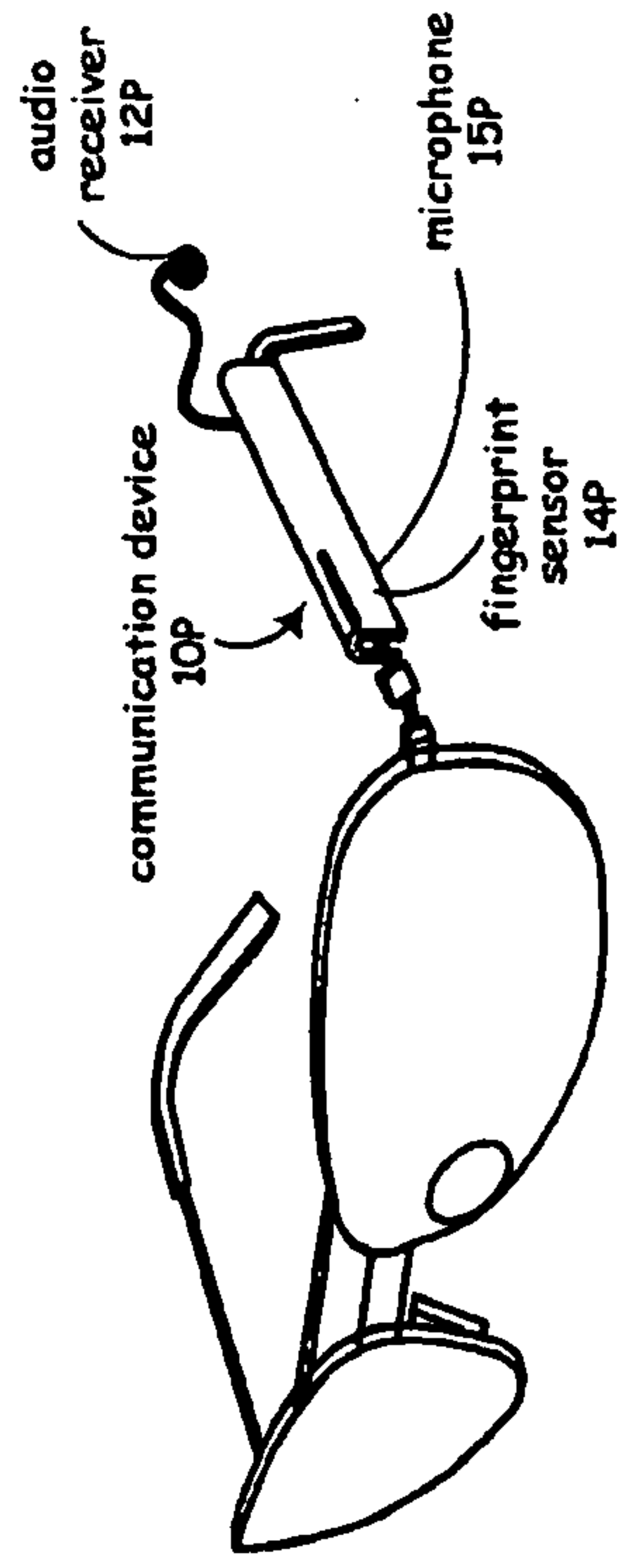


FIGURE 10B
GLASSES w/ WING
COMMUNICATION DEVICE

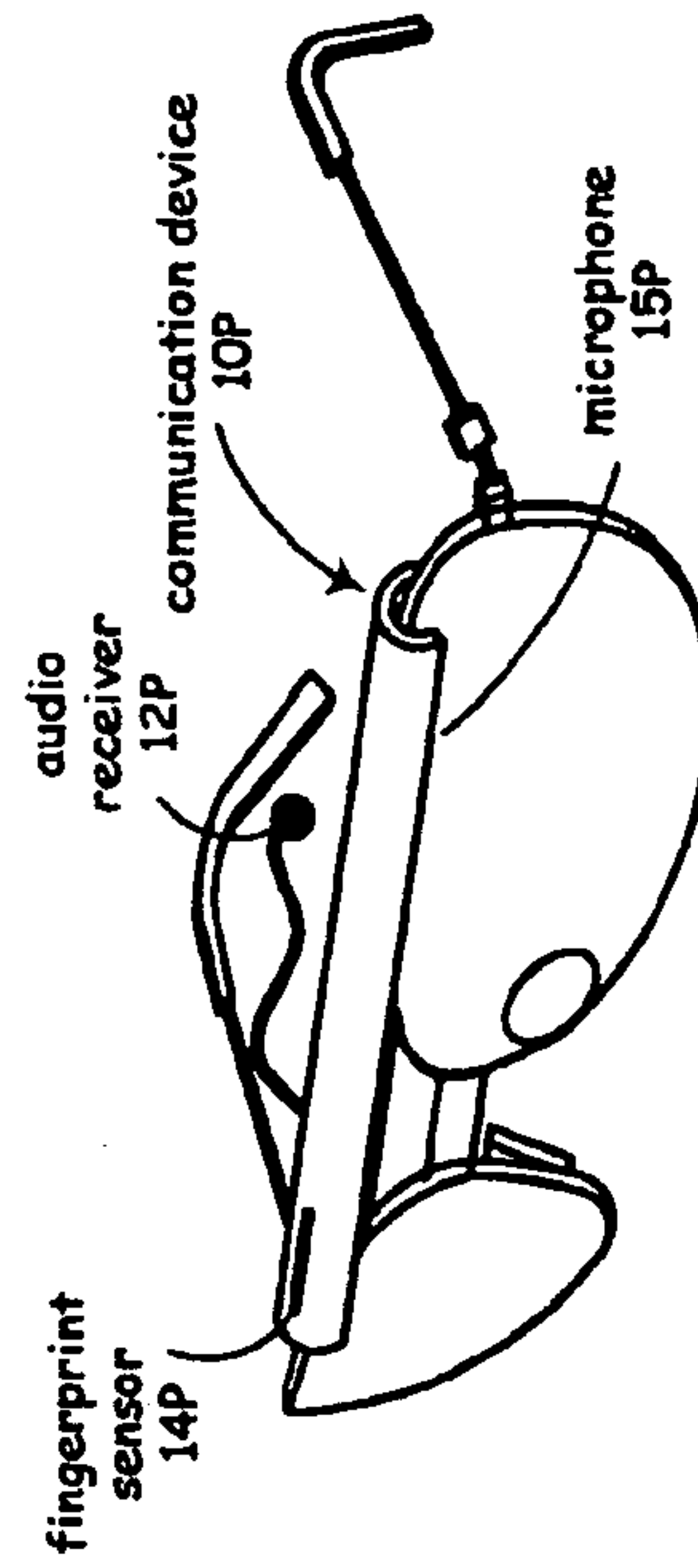
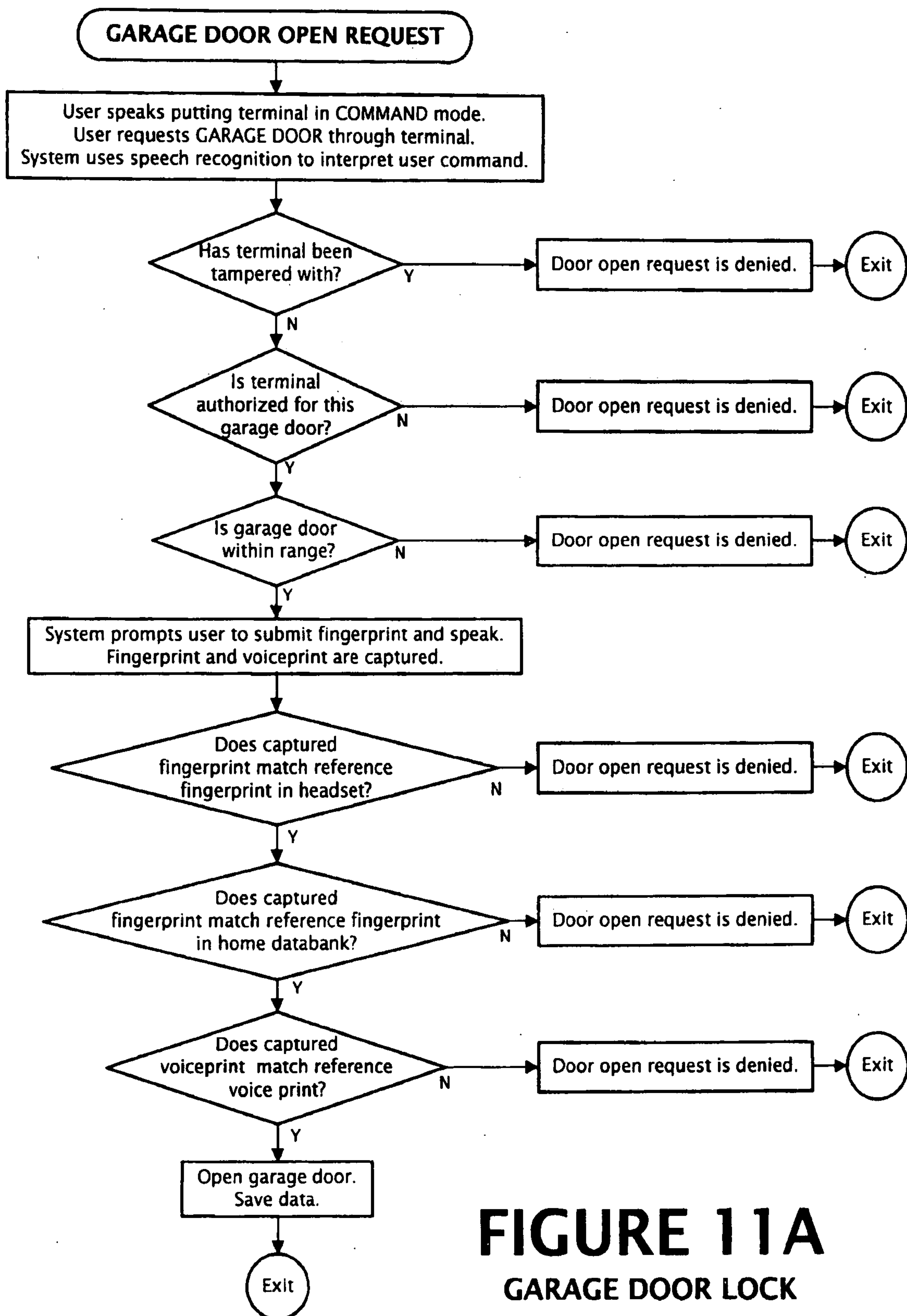


FIGURE 10C
GLASSES w/ FRAME
COMMUNICATION DEVICE



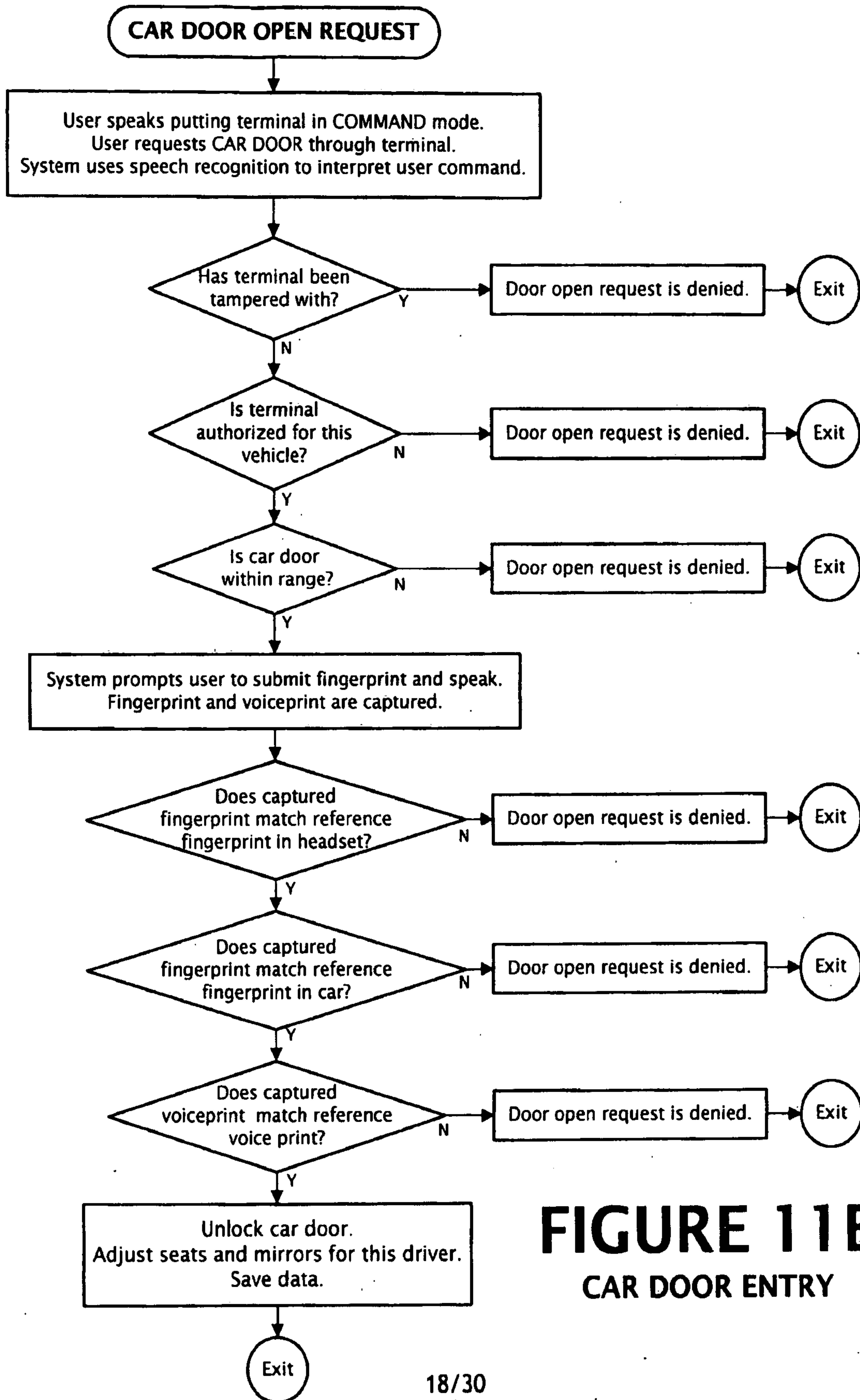


FIGURE 11B
CAR DOOR ENTRY

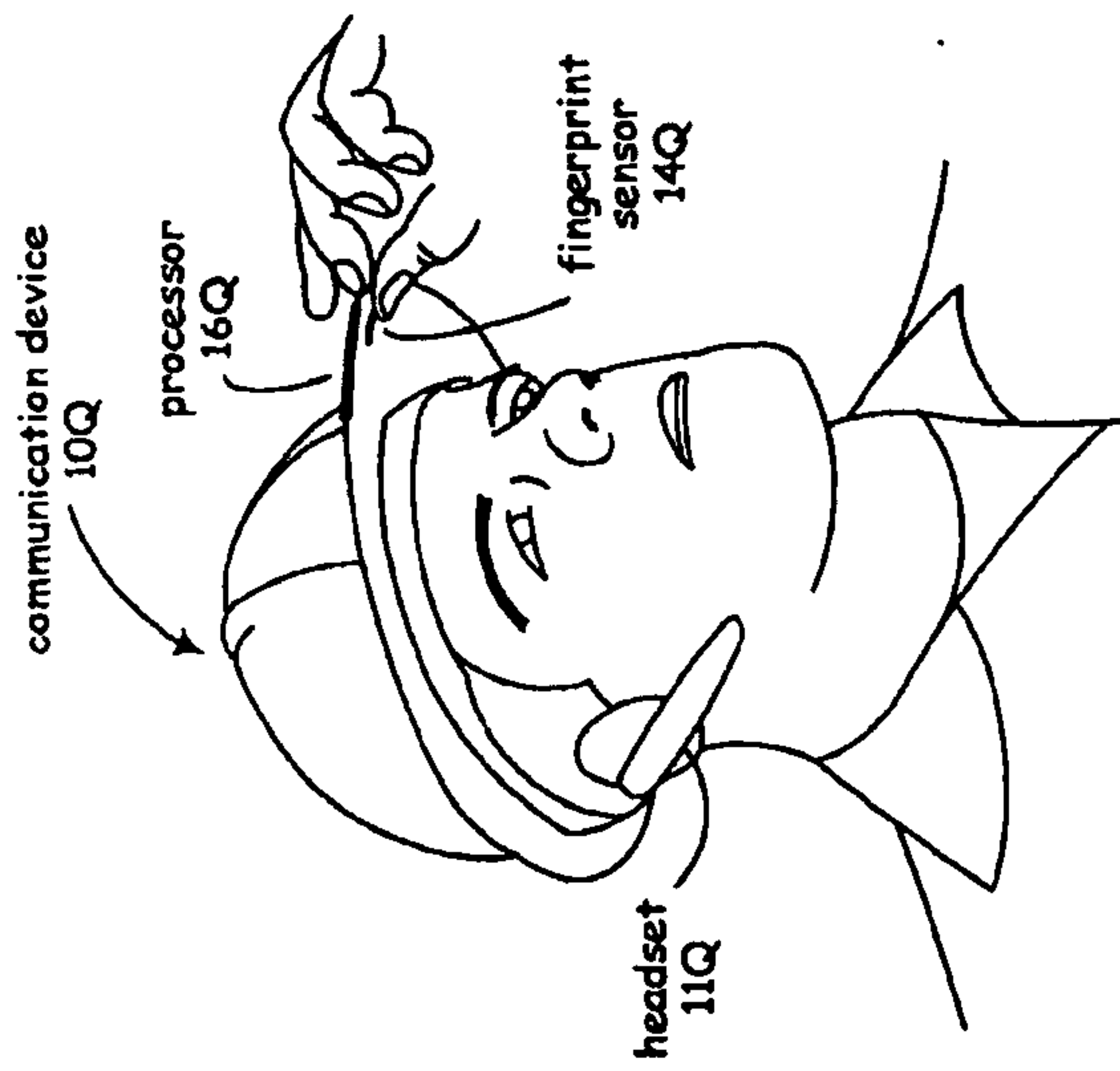


FIGURE 12A

SECURITY HEAD COVERING W/ SWEEP SENSOR

19/30

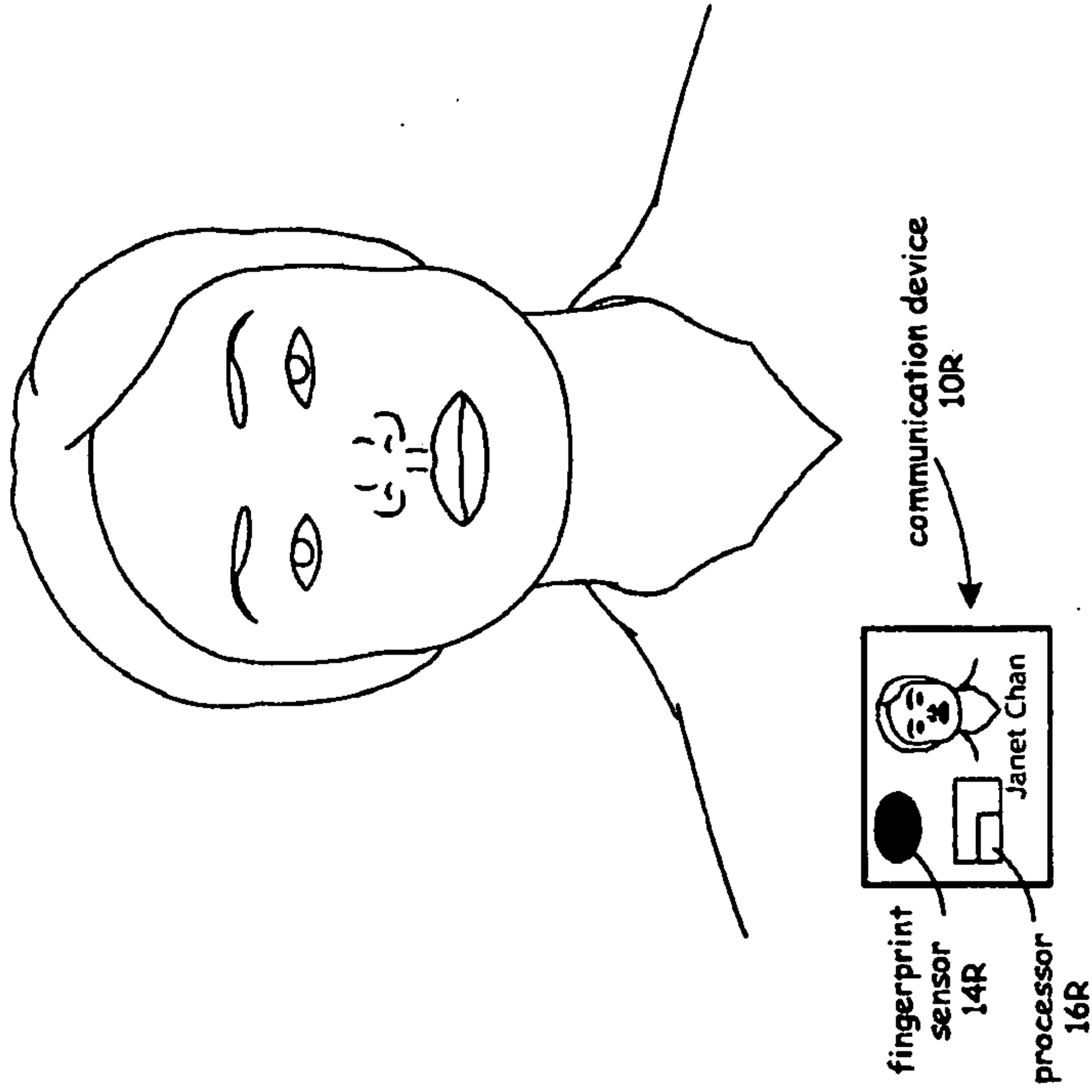


FIGURE 12B

SECURITY ID BADGE

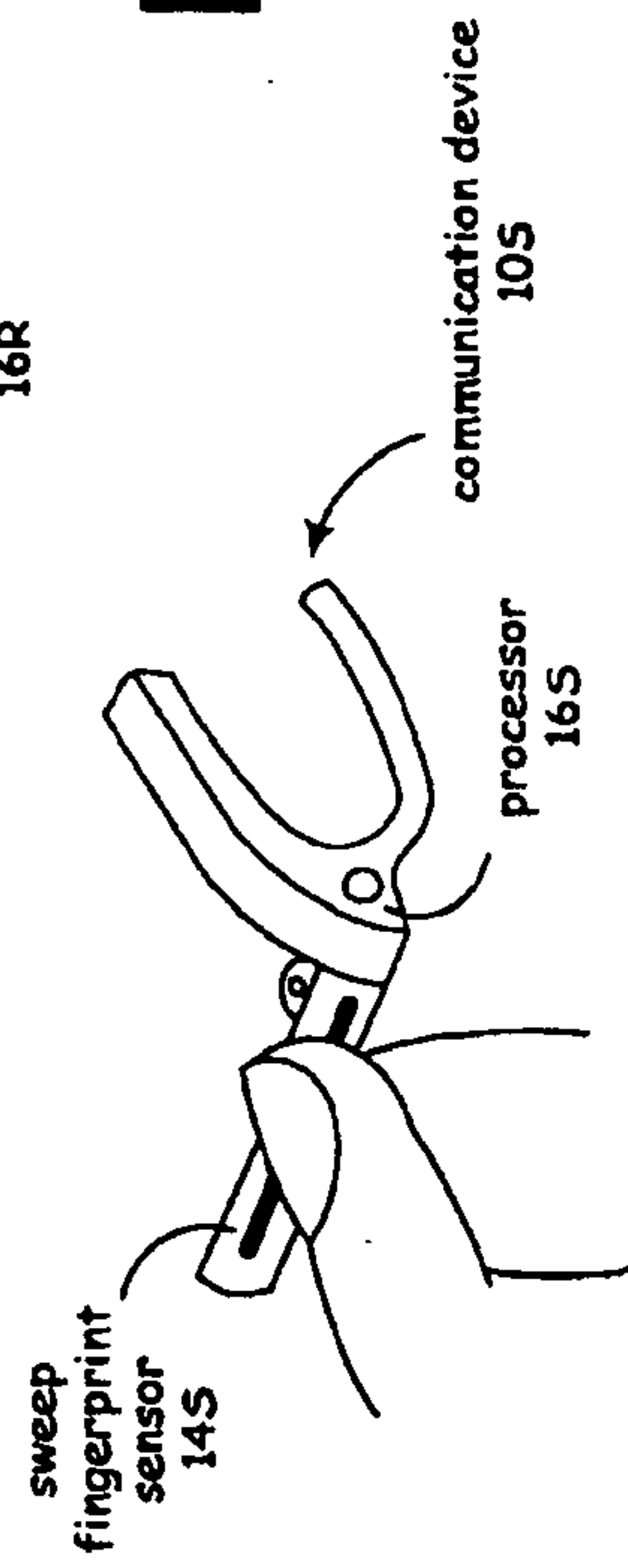


FIGURE 12C

SECURITY EYE-COVERING W/ SWEEP SENSOR

FIGURE 13A

ATM IDENTITY CONFIRMATION

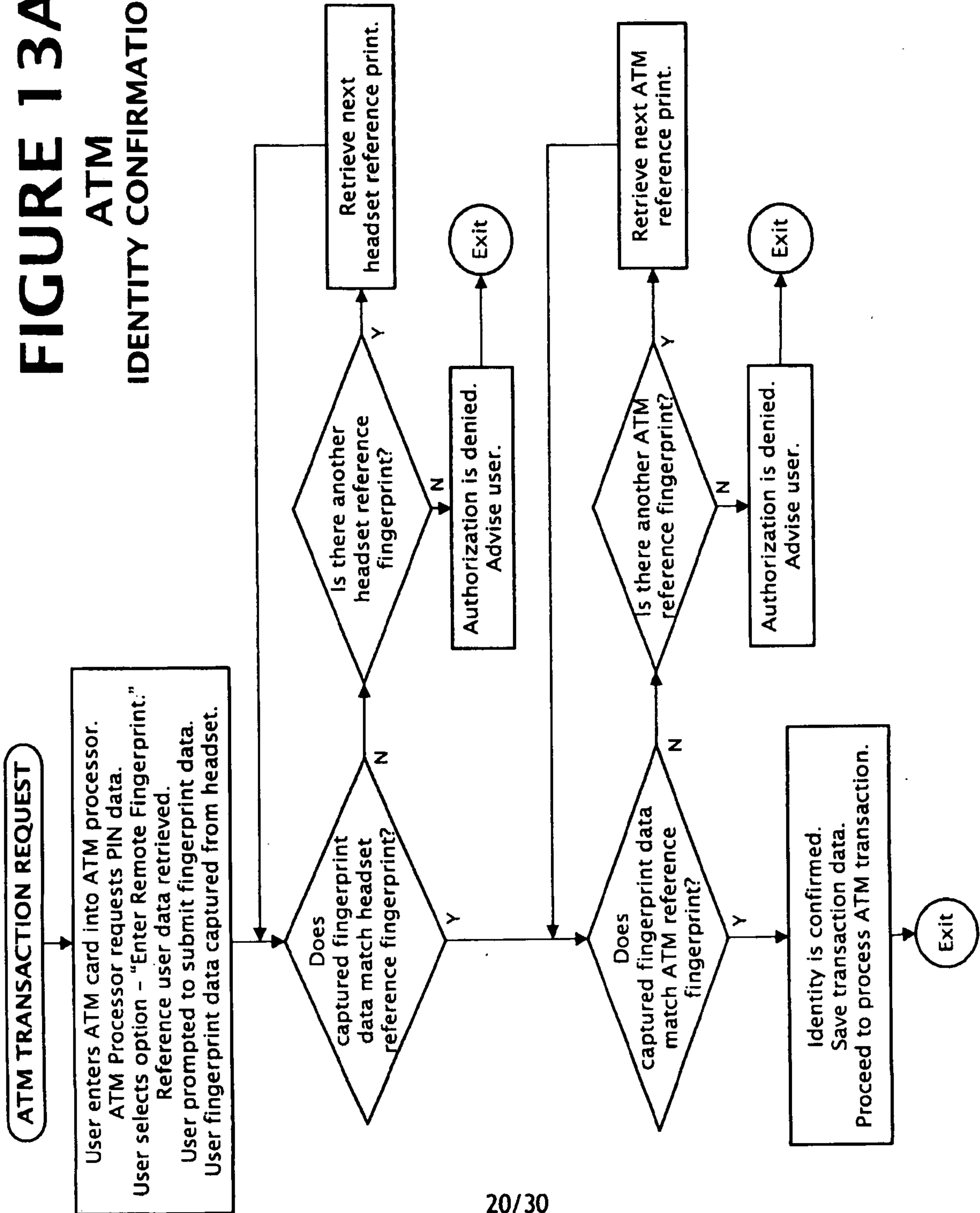
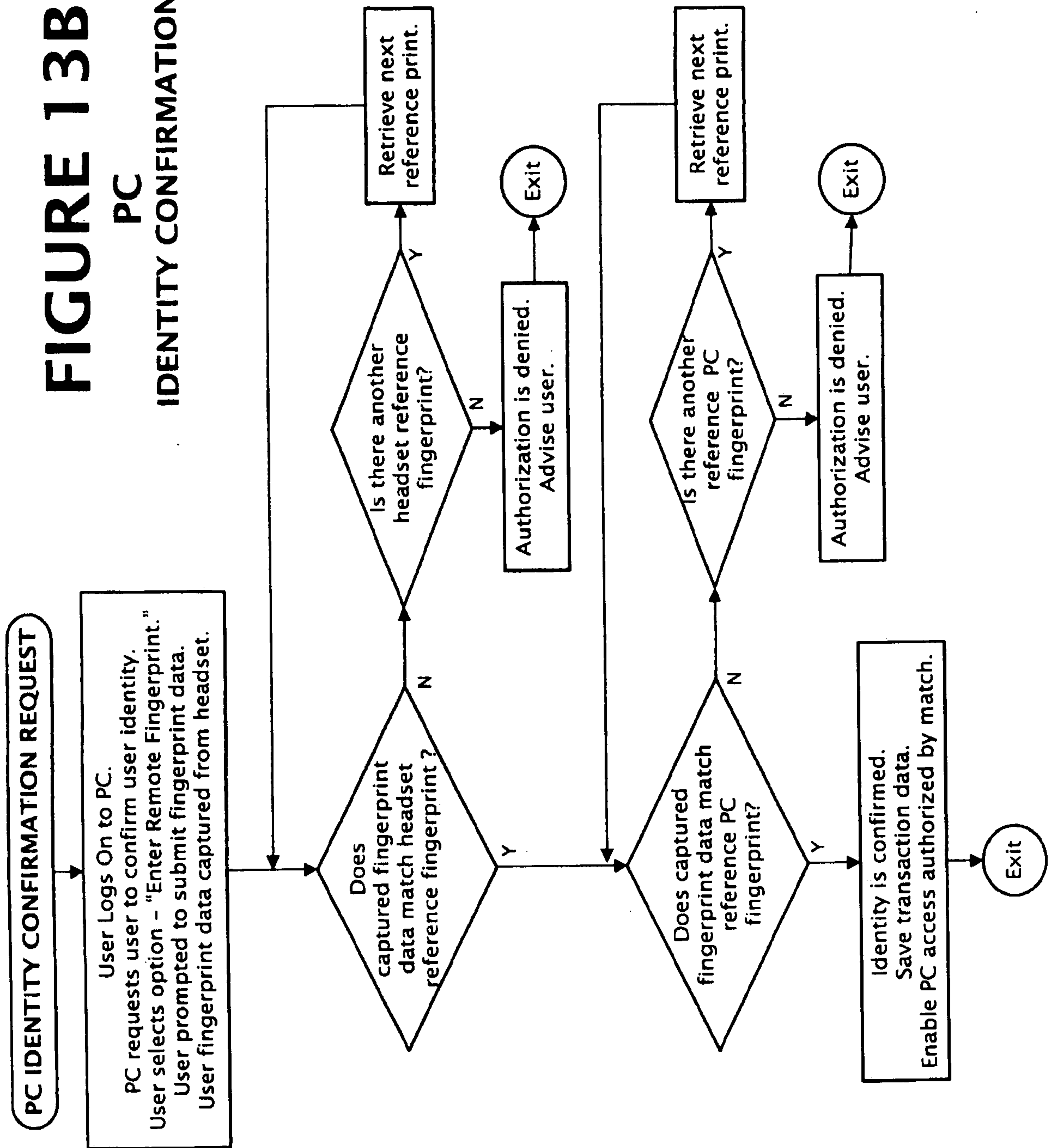
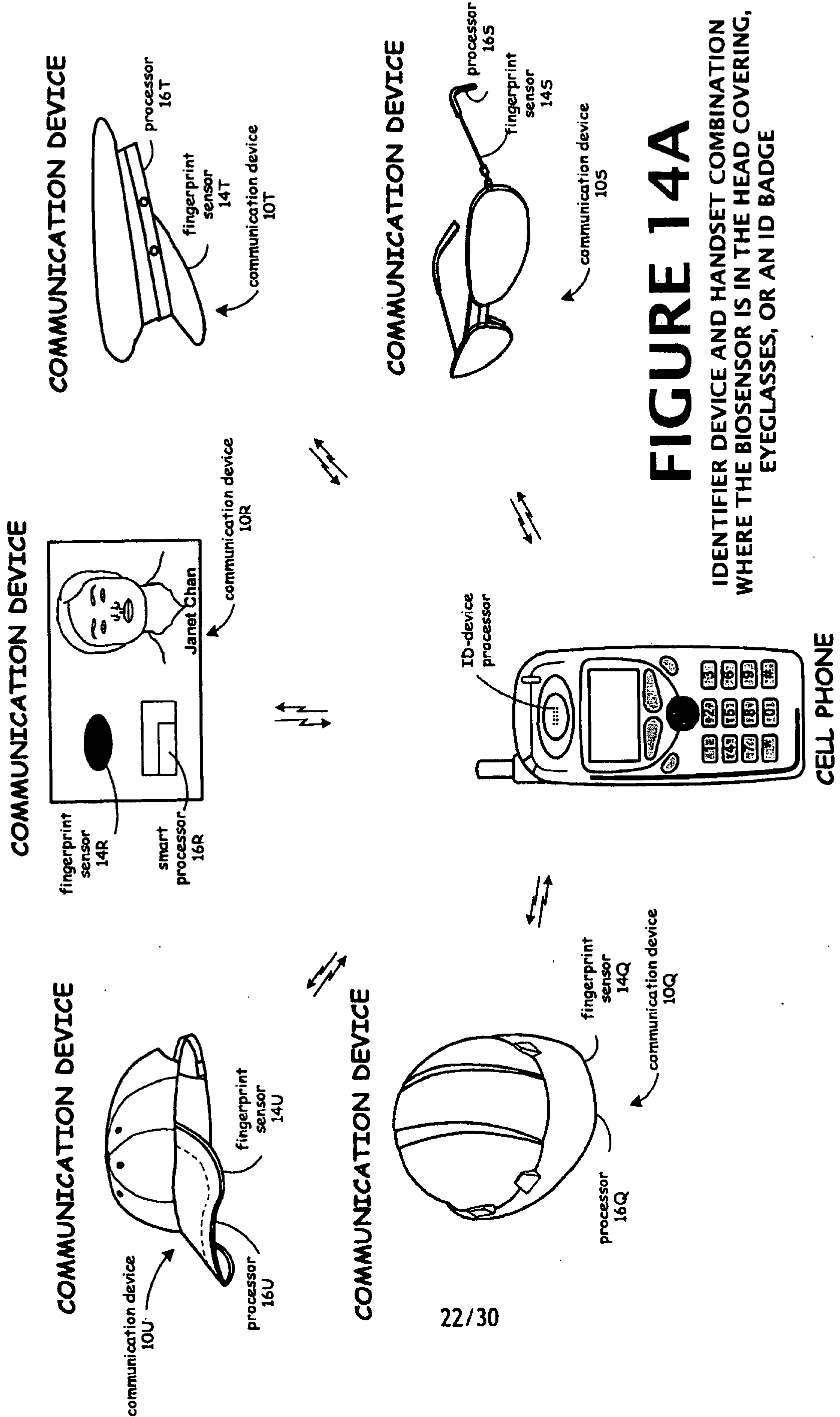


FIGURE 13B**PC****IDENTITY CONFIRMATION**



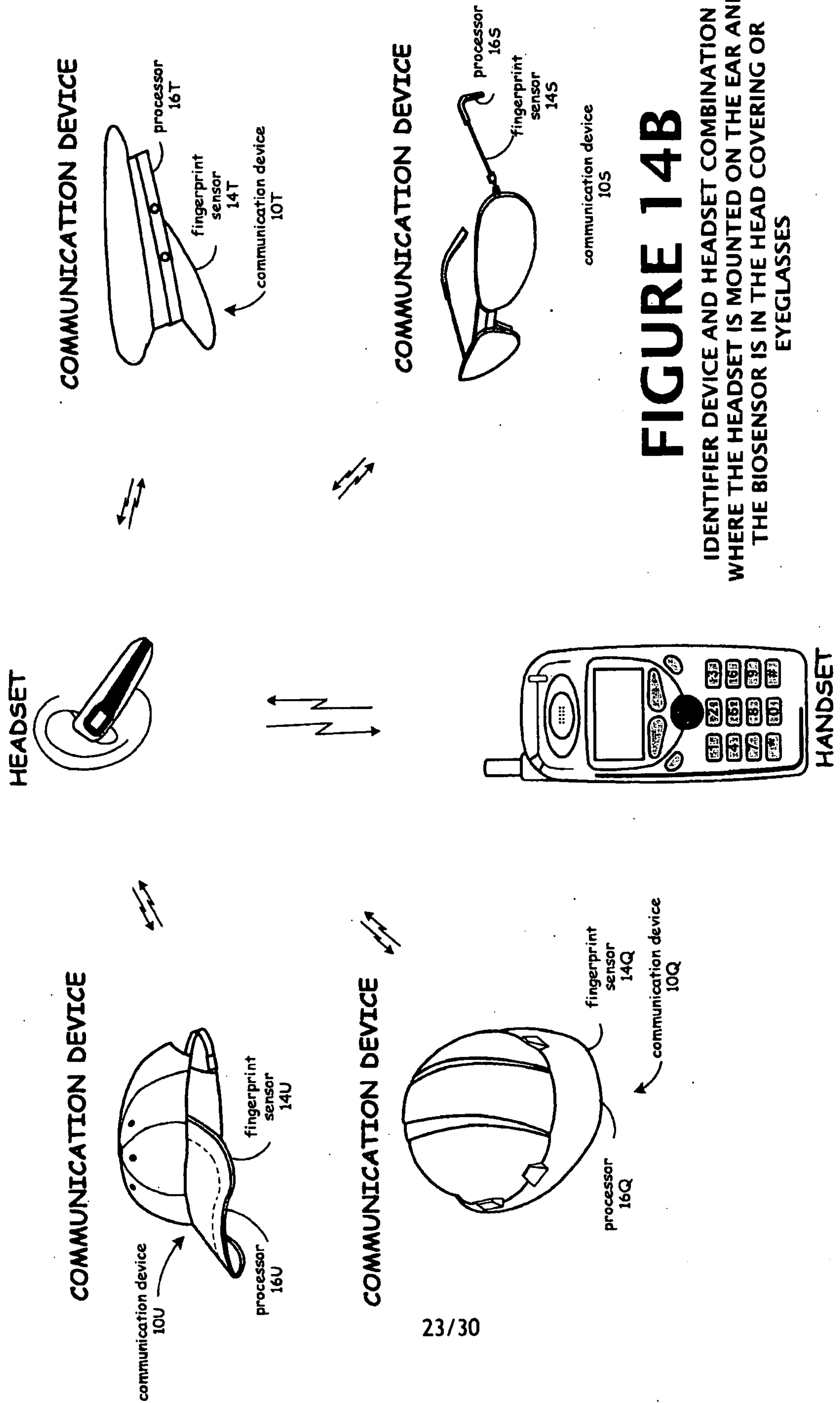


FIGURE 15A
IDENTIFIER DEVICE
PROCESSOR SCHEMATIC

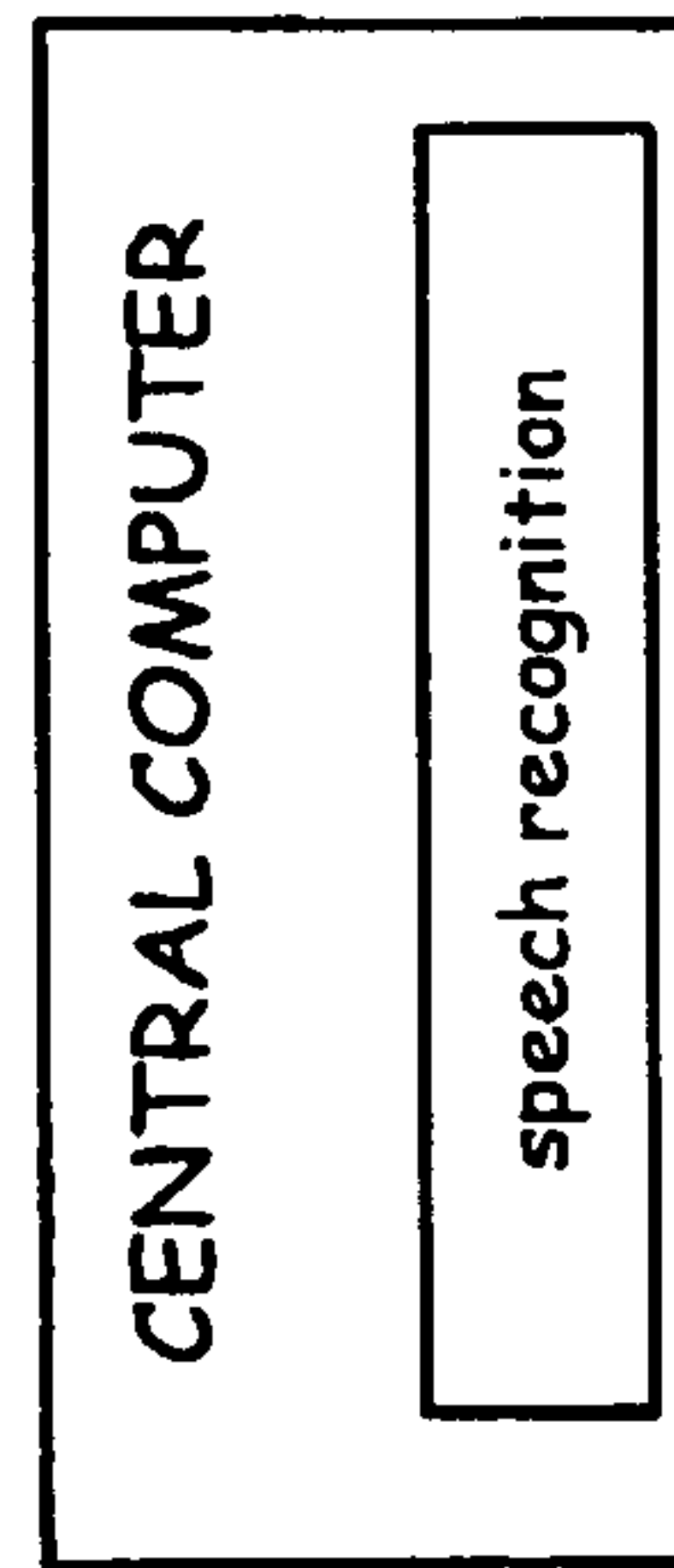
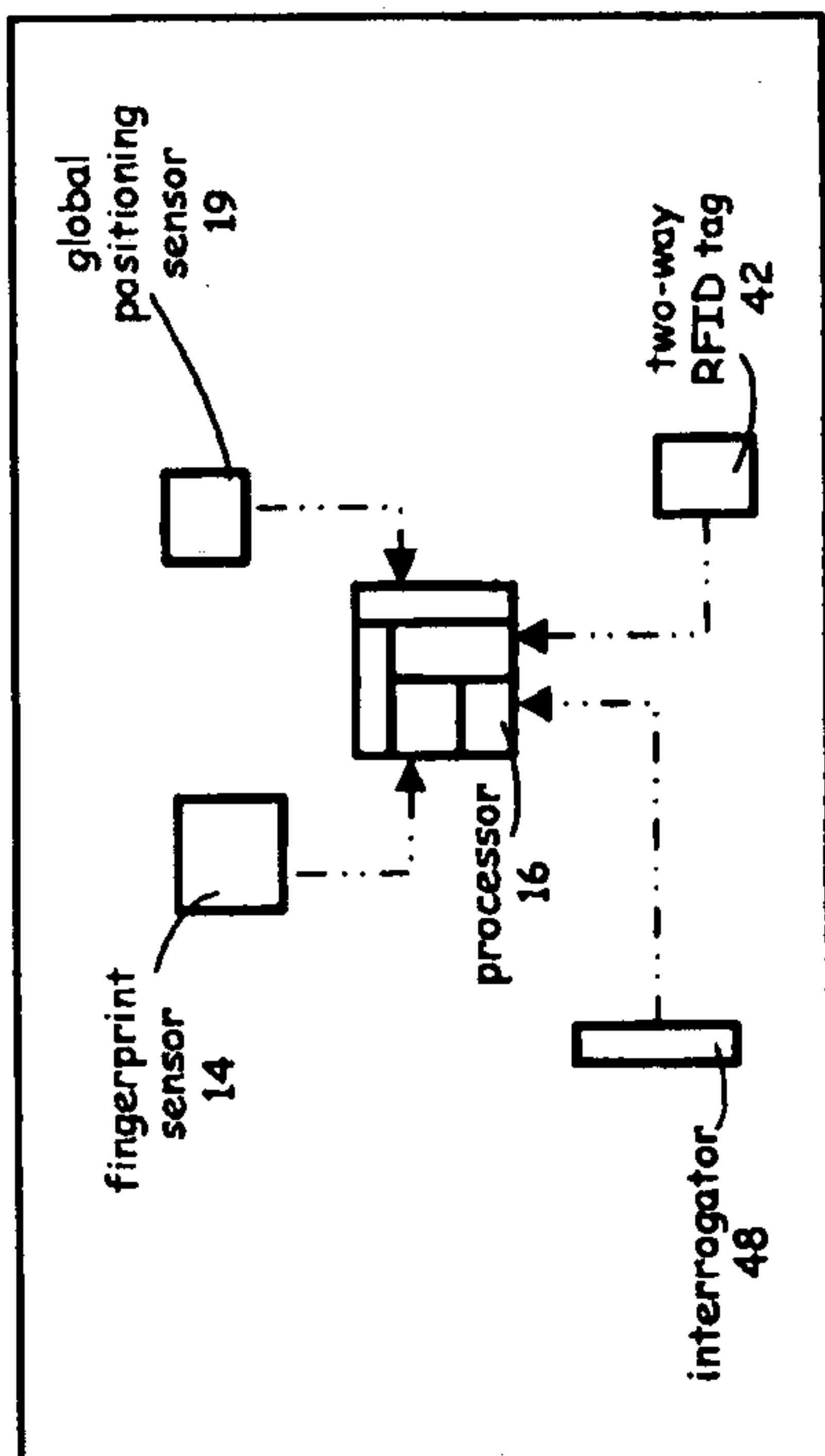
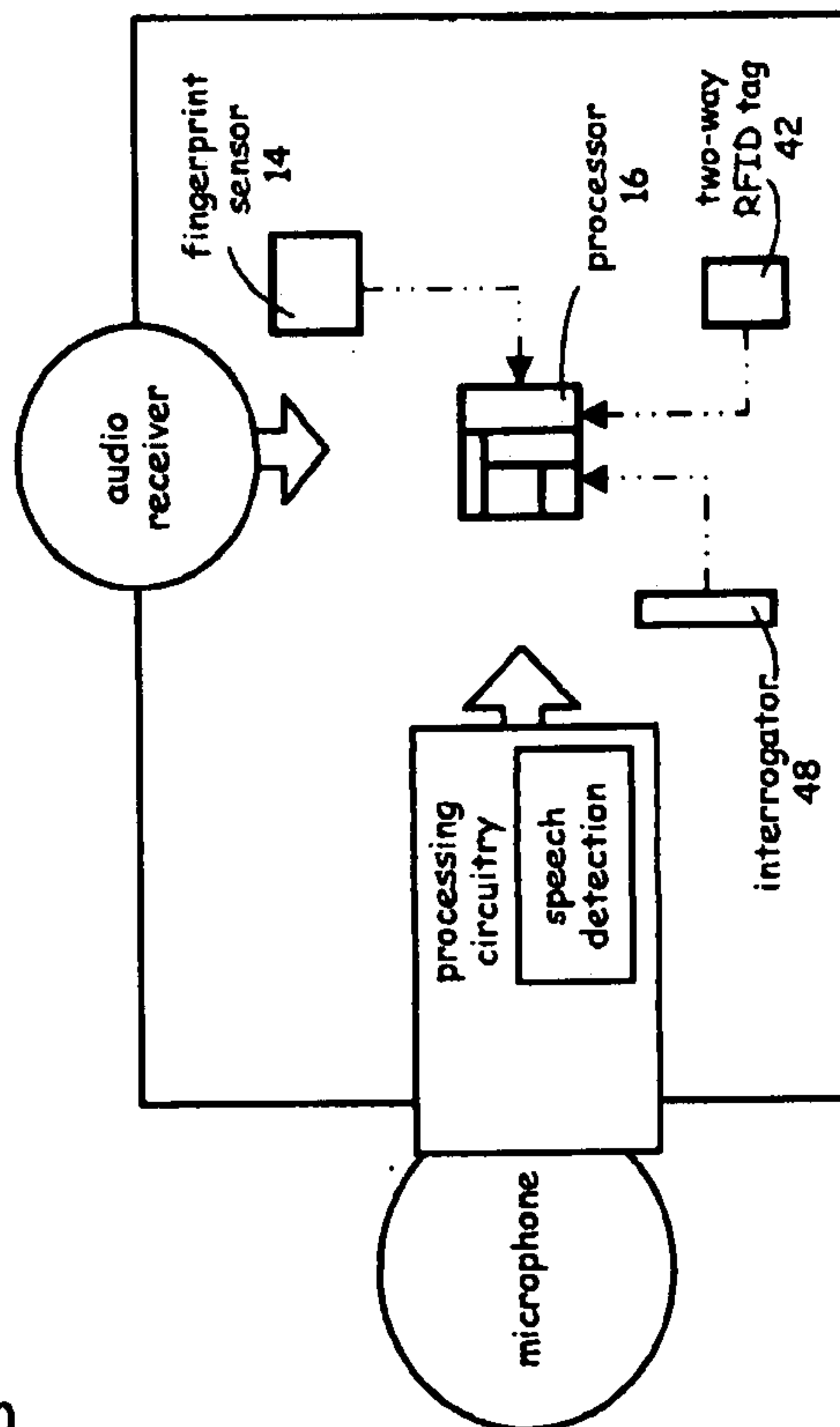


FIGURE 15B
COMMUNICATION DEVICE
PROCESSOR SCHEMATIC



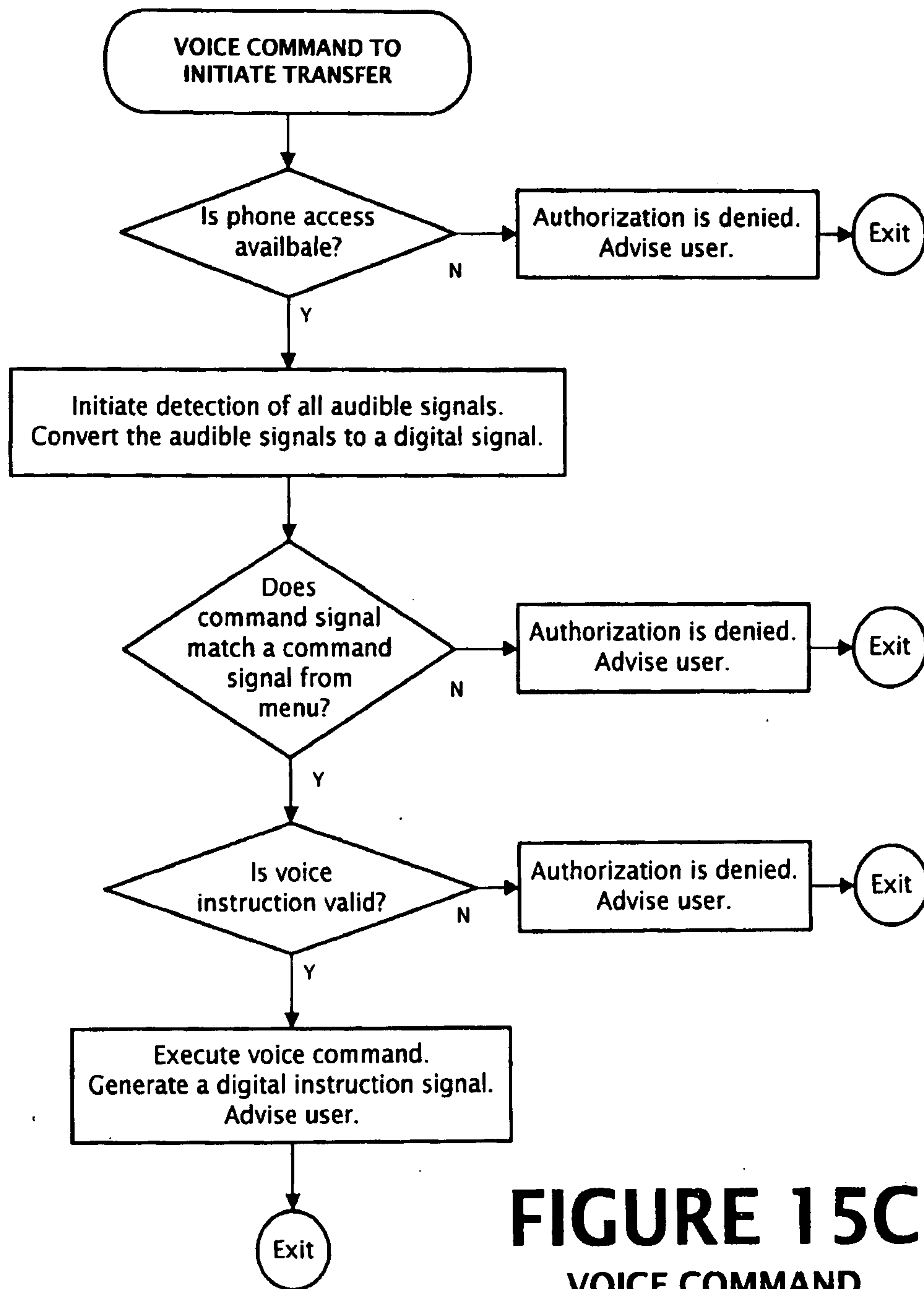
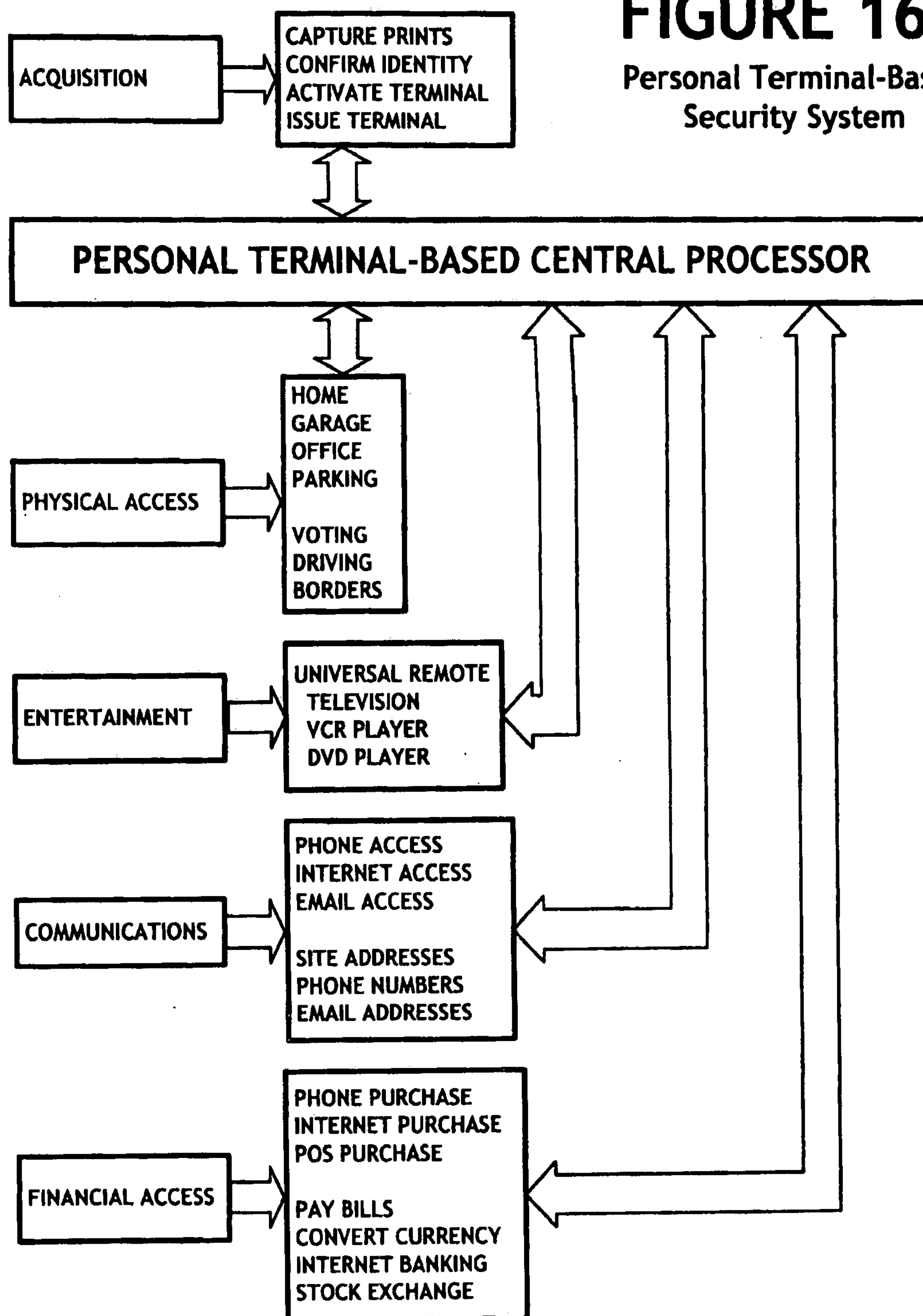
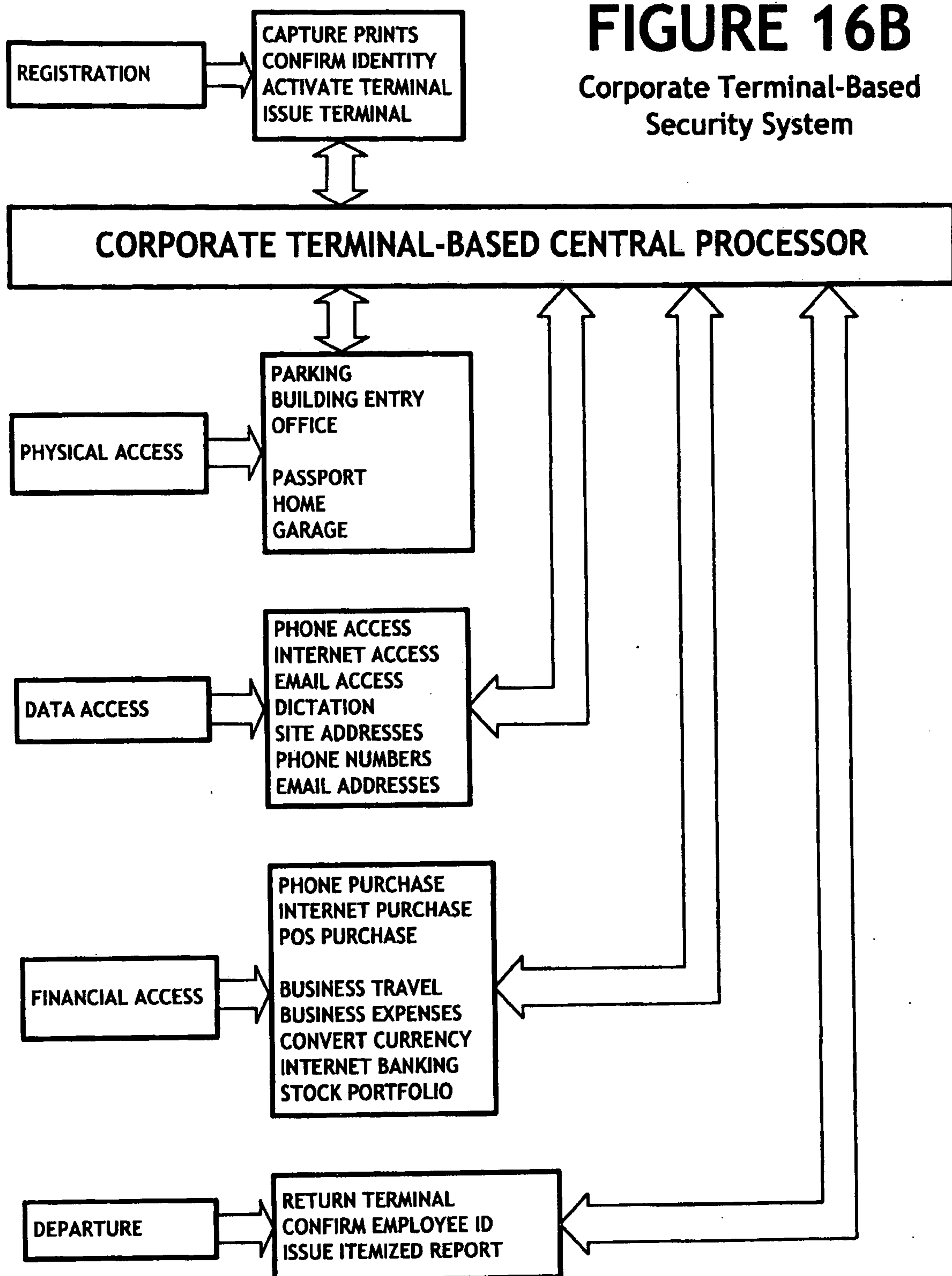
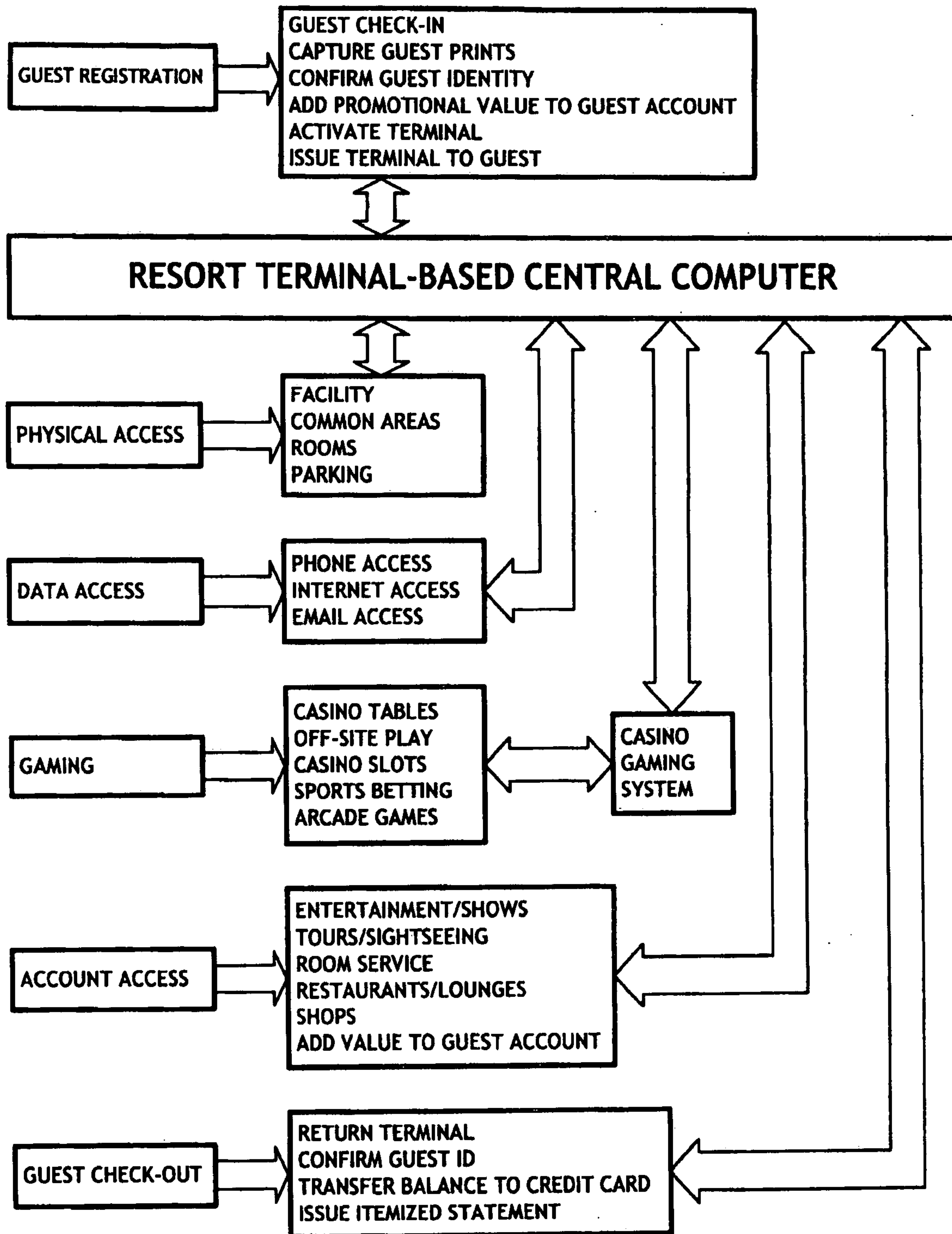


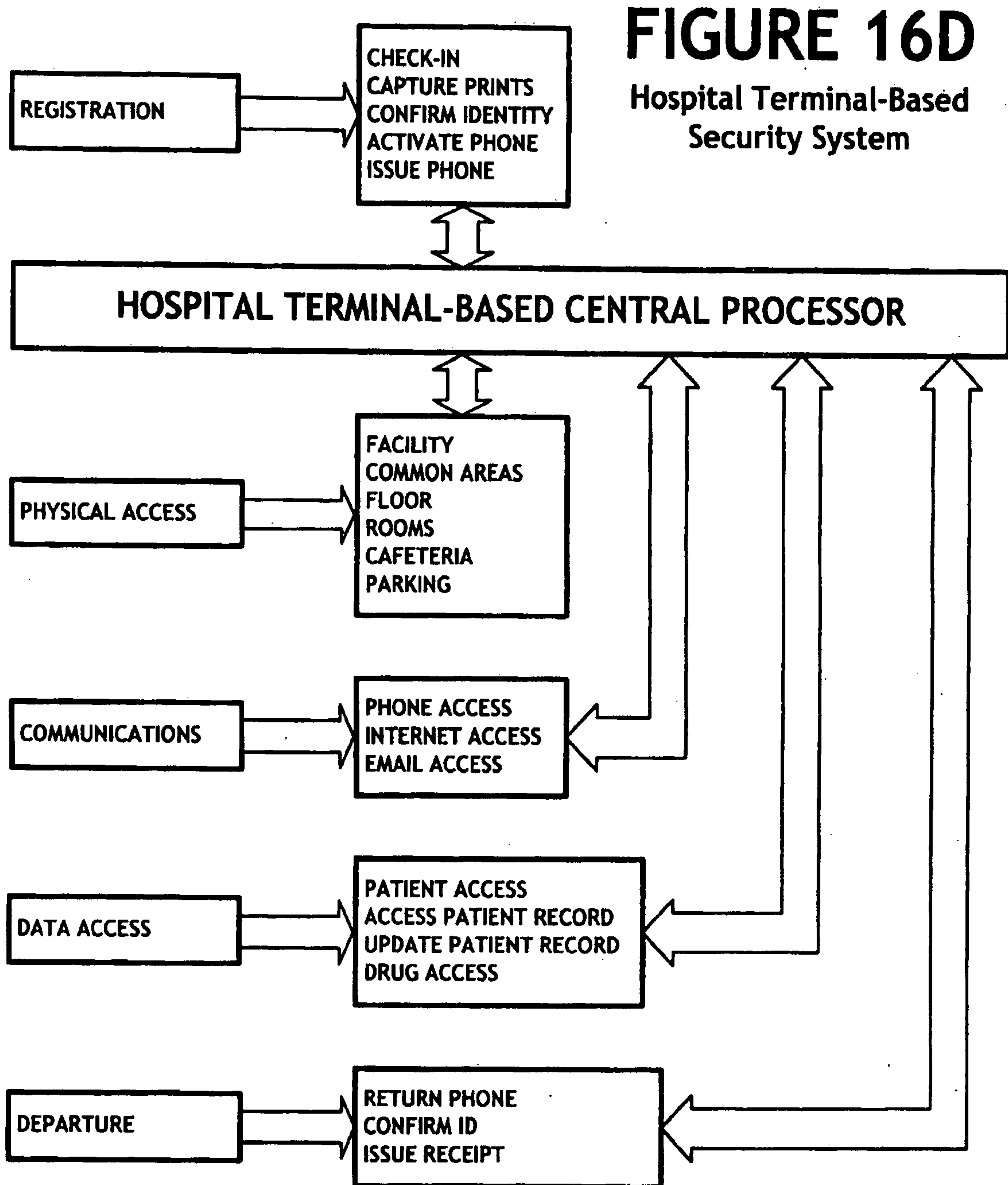
FIGURE 15C
VOICE COMMAND

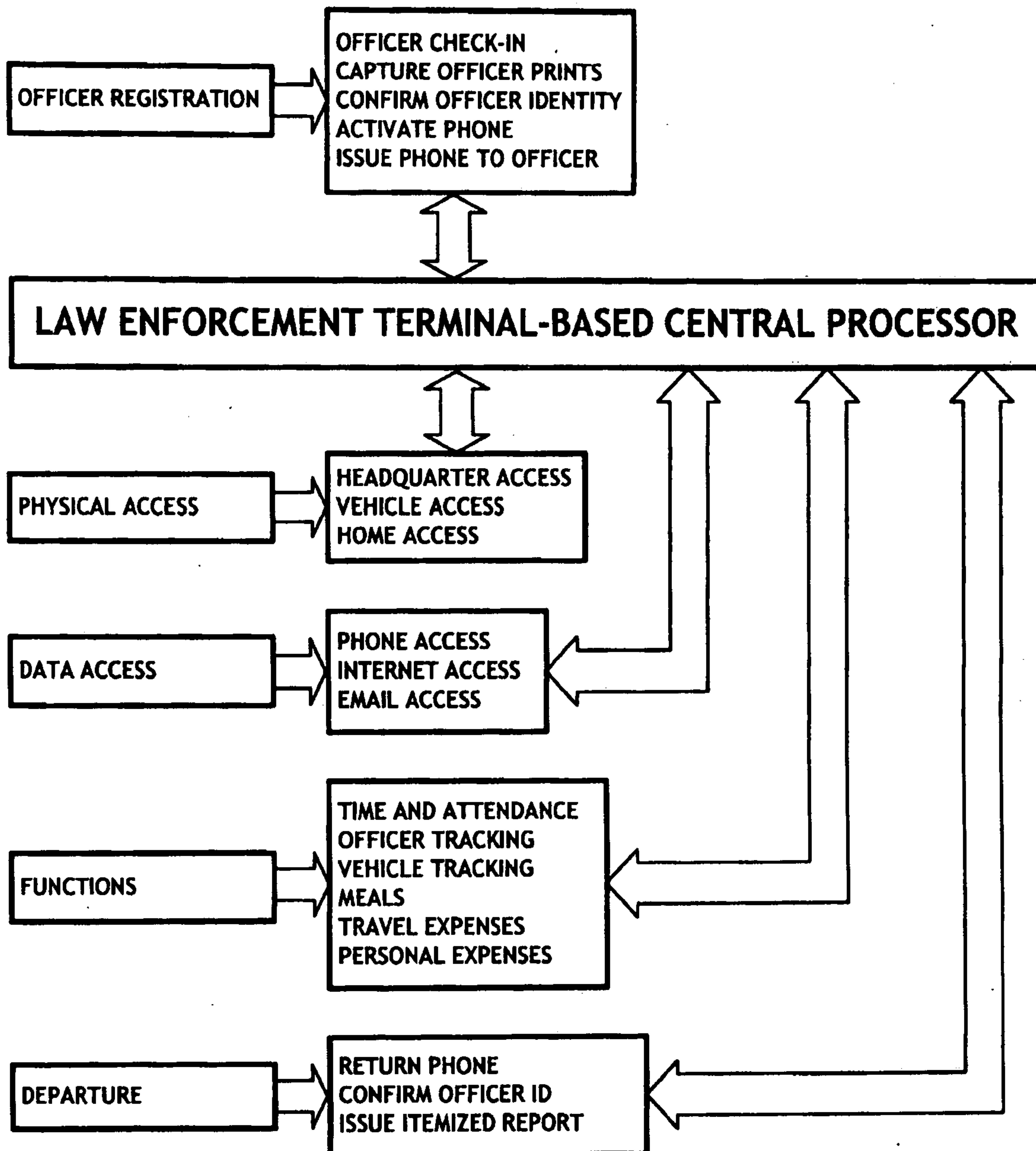
FIGURE 16A**Personal Terminal-Based
Security System**



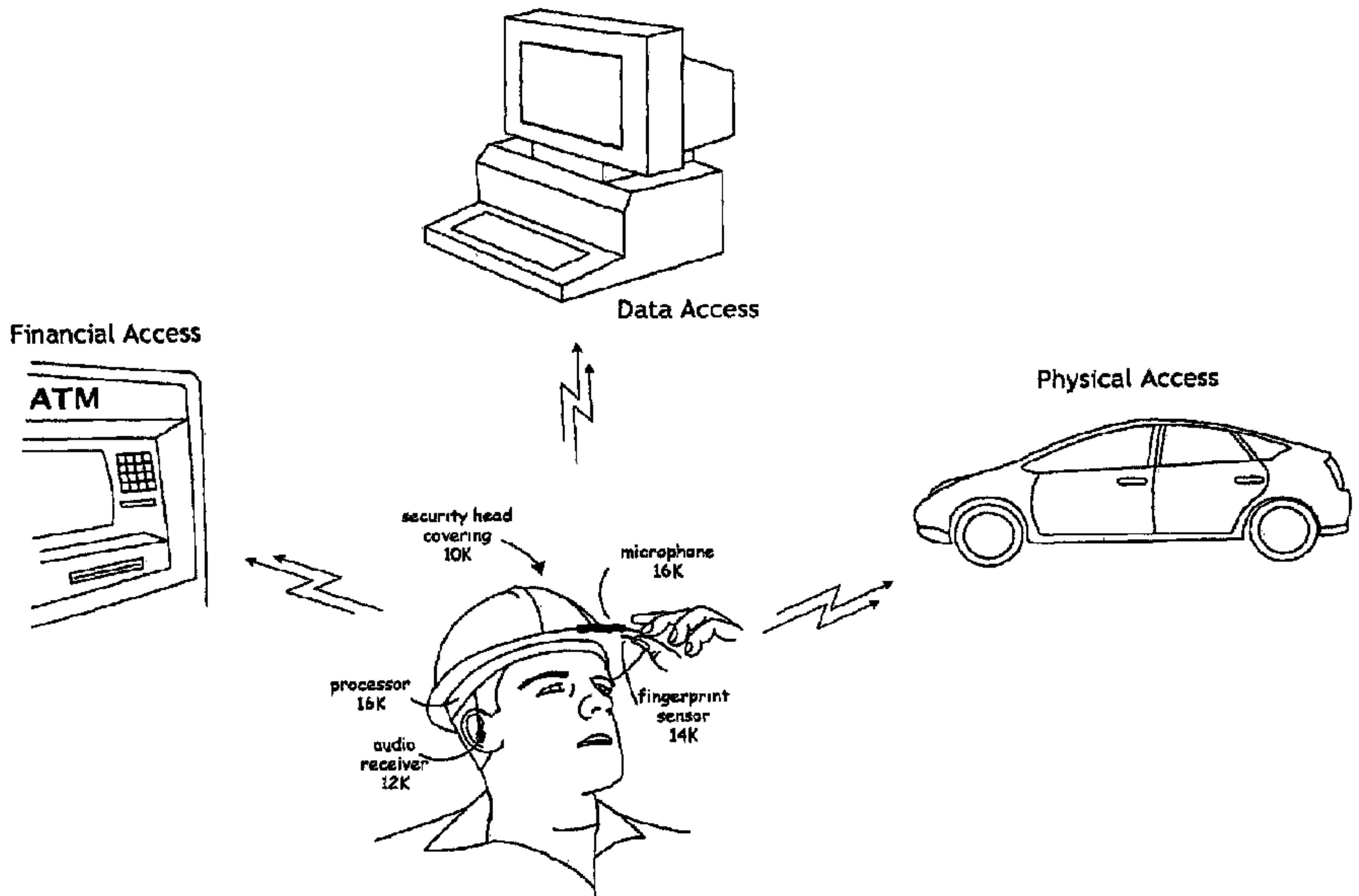
**FIGURE 16C**

Resort or Luxury Cruise
Terminal-Based Security System



**FIGURE 16E**

Law Enforcement Terminal-Based
Processing System



**FINGERPRINT SECURITY THROUGH A
HEADSET IN A HEAD COVERING**