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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2001 (27.09.2001)

PCT

(10) International Publication Number
WO 01/71671 A2

(51) International Patent Classification[7]: G07C 9/00, G06F 1/00

(21) International Application Number: PCT/US01/08962

(22) International Filing Date: 20 March 2001 (20.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/531,859 21 March 2000 (21.03.2000) US
09/531,720 21 March 2000 (21.03.2000) US

(71) Applicant: WIDCOMM, INC. [US/US]; Suite 205, 9645 Scranton Road, San Diego, CA 92121 (US).

(72) Inventor: MORRIS, Martin; 1055 Crestview Road, Vista, CA 92083 (US).

(74) Agents: ZIMMER, Kevin, J.; Cooley Godward LLP, 3000 El Camino Real, Five Palo Alto Square, Palo Alto, CA 94306-2155 et al. (US).

(81) Designated States *(national)*: CA, CN, DE, FI, GB, JP, MX, SE.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/71671 A2

(54) Title: SYSTEM AND METHOD FOR SECURE USER IDENTIFICATION WITH BLUETOOTH ENABLED TRANSCEIVER AND BIOMETRIC SENSOR IMPLEMENTED IN A HANDHELD COMPUTER

(57) Abstract: A system and method for secure biometric identification of the present invention. In a most general implementation, the inventive system includes a processor, a biometric sensor operationally coupled to the processor, and a wireless transmitter operationally coupled to the sensor. In the illustrative embodiment, the sensor is a fingerprint sensor and the transmitter is a wireless, Bluetooth enabled transceiver. The sensor and the transceiver are disposed on first and second expansion cards adapted to engaged an expansion slot of a Personal Digital Assistant.

SYSTEM AND METHOD FOR SECURE USER IDENTIFICATION WITH BLUETOOTH ENABLED TRANSCEIVER AND BIOMETRIC SENSOR IMPLEMENTED IN A HANDHELD COMPUTER

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to electronic devices and systems. More specifically, the present invention relates to systems and methods for providing user identification and/or authentication for electronic devices and systems.

Description of the Related Art

Currently, whenever a user wishes to access a computer-based system containing private data, the user must often identify himself, usually with a password. Passwords notoriously provide poor security as users either chose very simple, easily ascertained passwords or, if they use more difficult passwords, users often write them down, making them subject to theft.

In the end, most forms of encryption, as well as access controls such as passwords and even locks, serve a single purpose of identifying the person requesting access.

Hence, there is a need in the art for a reliable, secure system or method of authenticating the identity of a user. Ideally, the system or method would be effective such that one would not need to memorize passwords or utilize other authenticating devices such as keys to access computers and other electronic devices and systems.

SUMMARY OF THE INVENTION

The need in the art is addressed by the system and method for secure biometric identification of the present invention. In a most general implementation, the inventive system includes a processor, a biometric sensor operationally coupled to the processor, and wireless transmitter operationally coupled to the sensor.

In the illustrative embodiment, the processor is the central processing unit of a Personal Digital Assistant (PDA). In the preferred embodiment, the PDA is equipped with an expansion slot allowing access to the system bus thereof. The sensor is a fingerprint sensor and the transmitter is a wireless, Bluetooth enabled transceiver. The sensor and the transceiver are disposed on first and second expansion cards designed to engage the expansion slot of a Personal Digital Assistant and connect to the system bus.

The inventive system provides a mobile, secure and inexpensive system and technique for providing biometric data for user authentication and identification.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a perspective view of a PDA suitable for use in connection with the teachings of the present invention.

Fig. 2 is a perspective rear view of a portion of a PDA equipped with an expansion slot with a card partially inserted therein.

Fig. 3 is a block diagram of an illustrative implementation of a PDA with a biometric sensor constructed in accordance with the present teachings.

Fig. 4 is a schematic diagram showing illustrative interfacing details between the card and the PDA.

Fig. 5 is a flow diagram illustrative of a method of using the PDA with biometric sensor of the present invention. Fig. 5(a) shows an illustrative startup routine for the card

utilized in the PDA of the illustrative embodiment. Fig. 5(b) shows a method for using the fingerprint sensor of the illustrative embodiment.

DESCRIPTION OF THE INVENTION

Illustrative embodiments and exemplary applications will now be described with reference to the accompanying drawings to disclose the advantageous teachings of the present invention.

While the present invention is described herein with reference to illustrative embodiments for particular applications, it should be understood that the invention is not limited thereto. Those having ordinary skill in the art and access to the teachings provided herein will recognize additional modifications, applications, and embodiments within the scope thereof and additional fields in which the present invention would be of significant utility.

As mentioned above, and in accordance with the present teachings, the inventive system includes a Personal Digital Assistant (PDA) adapted to receive biometric input from a fingerprint sensor and provide a first signal in response thereto. Personal Digital Assistants are well known and widely used.

Fig. 1 is a perspective view of a PDA suitable for use in connection with the teachings of the present invention. The PDA 10 is shown resting in a cradle 11. As is well known in the art, the PDA 10 is a handheld computer having a liquid crystal display and touchscreen 12 and a keypad 14. As discussed more fully below, in the best mode, the PDA 10 is equipped with an expansion slot such as the Visor$_{tm}$ Handheld Computer manufactured and sold by Handspring and disclosed more fully at www.handspring.com.

Fig. 2 is a perspective rear view of a portion of a PDA 10 equipped with an expansion slot 15 with a card 16 partially inserted therein. (The images depicted in Figs. 1 and 2 are copyrighted by Handspring and shown merely to illustrate a commercially

available PDA adapted for use with the present invention and how a card may be constructed in accordance with the present teachings and utilized with the PDA respectively. Applicant makes no claim of inventorship with respect to the PDA 10 or cradle 11.)

In accordance with the present teachings, a biometric device, in the illustrative embodiment - a fingerprint sensor 18, is disposed on the card 16. In the illustrative embodiment, the fingerprint sensor 18 is centered on the card 16 and located a distance 'd' from the top of the card so that when the PDA is held, an index finger of either hand is naturally and comfortably applied to the sensor. Those skilled in the art will appreciate that the invention is not limited to the location of the sensor or the type of sensor used. The sensor 18 may sense any biometric data including body temperature, skin conductivity, voice data, eye pupil data etc.

The fingerprint sensor of the illustrative embodiment may be purchased from Veridicom, Inc. of Santa Clara, CA as a model FPS110 sensor. This sensor is particularly well suited for the present application in that it senses a change in capacitance associated with a given fingerprint as opposed to an optical image. Accordingly, system design is simplified by eliminating optics and the fingerprint is not easily forged with a printed copy. When the card is inserted into the expansion slot, it interfaces electrically with the system bus of the PDA and completes the electrical circuit depicted in Fig. 3.

Fig. 3 is a block diagram of an illustrative implementation of a PDA with a biometric sensor constructed in accordance with the present teachings. The system 20 includes the PDA 10 and the card 16. In accordance with the present teachings, a wireless transceiver 22 is disposed on the card 16. In the preferred embodiment, the transceiver 22 is adapted to operate in accordance with the BLUETOOTH SPECIFICATION VERSION 1.0A CORE, published in July 1999. The wireless transceiver 22 is connected to an antenna 24 and communicates with a central processing unit (CPU) 26 of the PDA 20 via a bus 25.

In an illustrative embodiment, the fingerprint sensor 18 is mounted on a secondary card 21, which is adapted to interface with the primary card 16.

Fig. 4 is a schematic diagram showing illustrative interfacing details between the card and the PDA. In the illustrative implementation, the bus 25 provides 24 address lines and a 16 bit data bus. 'csSlot0' and 'csSlot1' are control signals while 'CD1' and 'CD2' are card detection signals. 'Vdock' provides module charging power from the cradle 11.

A flash memory circuit is provided on the card 16 to provide application specific information to the CPU via the bus 25. The flash memory is read-only memory (ROM) and contains module header information and any other applications needed for the module or card 16. The application stored in the memory 16 includes drivers for the sensor 18 and would be created with a utility provided in a developer's kit supplied by the manufacturer, e.g., the "Palm-makeROM" utility included in the Springboard Developer's Kit supplied by Handspring. In the illustrative embodiment, the CPU 26 runs with a standard Palm® <is "Palm" the trademark or "PalmOS"?>operating system. After the system 10 is initialized, the central processing unit 26 receives biometric data from the fingerprint sensor 18 via the bus 25. See Fig. 3.

Those skilled in the art will appreciate that the system 20 affords many modes of operation. For example, the biometric data, i.e., fingerprint data in the illustrative embodiment, may be encrypted in hardware (not shown) or in software via control software provided by the flash memory 28 or an internal memory 30 provided in the PDA 10. The encrypted biometric data may then be transmitted to a remote server for authentication and identification as depicted in the flow diagram of Fig. 5.

(Encryption hardware and software are well known in the art. See for example U.S. Patent No. 4,405,829 entitled Cryptographic communication system and method, issued 9/20/83 to Rivest, et al. the teachings of which are incorporated herein by reference. As will be readily apparent to those skilled in the art, the control software also enables the CPU 26 to selectively access and control the mobile unit components via a system bus shown generally at 25.

Fig. 5 is a flow diagram illustrative of a method of using the PDA with biometric sensor of the present invention. Fig. 5(a) shows an illustrative startup routine for the card 16 such as that utilized by the Visor® PDA sold by Handspring. At step 104, the system 20

checks for an interrupt indicating module detection. If the module 16 is detected, then at step 106, the module is powered up slowly. At step 108, the operating system reads the module header and updates the application launcher globals. That is, the operating system maps the chip select signals to the default address range, resets the module and checks the card header. If the card header is valid, the operating system registers the card or module 16.

At step 110, the operating system checks for a 'setup app' signal indicating the presence of an application on the module 16. If an application is present, at step 112, the operating system makes a copy and executes the application. If, at step 114, a 'welcome app' signal is present, then at step 116, the welcome application is executed directly from the module memory 28. In any case, at step 118, all applications appear in the applications launcher and the method continues in Fig. 5(b).

Fig. 5(b) shows a method for using the fingerprint sensor of the illustrative embodiment. As shown in Fig. 5(b), the system 20 waits in a standby mode for biometric data at steps 120 and 122. When the data is available, it is encrypted at step 124 and transmitted at step 126.

Those skilled in the art will appreciate that as an alternative, the fingerprint may be authenticated in the system 20 in which case, a secure resource provided at the PDA might then be made accessible. A system and method in accordance with this implementation is disclosed and claimed in copending U.S. utility Application No. 09/531,720 filed on March 21, 2000, entitled "SYSTEM AND METHOD FOR SECURE BIOMETRIC IDENTIFICATION", inventor Martin Morris (Attorney Docket No. WIDC-012/00US) the teachings of which are incorporated herein by reference.

As yet another alternative, on validation of the fingerprint, a key or other message may be transmitted to a remote device or network via the wireless link. In any case, it is contemplated that two or more prints may be stored for a given user.

Thus, the present invention has been described herein with reference to a particular embodiment for a particular application. Those having ordinary skill in the art and access

to the present teachings will recognize additional modifications applications and embodiments within the scope thereof.

It is therefore intended by the appended claims to cover any and all such applications, modifications and embodiments within the scope of the present invention.

Accordingly,

WHAT IS CLAIMED IS:

1. Apparatus for use in a system for secure identification comprising:
a processor;
a biometric sensor operationally coupled to said processor; and
wireless transmitter operationally coupled to said sensor.

2. The invention of Claim 1 wherein said transmitter is a wireless transceiver.

3. The invention of Claim 2 wherein said transceiver is a Bluetooth enabled transceiver.

4. The invention of Claim 3 wherein said sensor is a fingerprint sensor.

5. The invention of Claim 4 further including a computer of which said processor is a central processing unit.

6. The invention of Claim 5 wherein said computer is a handheld computer.

7. The invention of Claim 6 wherein said computer is a Personal Digital Assistant.

8. Apparatus for use in a system for secure identification comprising:
a handheld computer and
a biometric sensor electronically connected to said handheld computer.

9. The invention of Claim 8 wherein said biometric sensor is a fingerprint sensor.

10. The invention of Claim 9 further including a wireless transceiver.

11. The invention of Claim 10 wherein said handheld computer is a personal digital assistant.

12. The invention of Claim 11 wherein said computer includes a central processing unit.

13. The invention of Claim 11 further including a system bus electrically connected to said computer.

14. The invention of Claim 13 wherein said handheld computer has an expansion slot.

15. The invention of Claim 14 wherein said apparatus further includes a first card adapted to physically engage said expansion slot.

16. The invention of Claim 15 wherein said transceiver is disposed on said first card.

17. The invention of Claim 16 further including a second card adapted to electrically connect to said first card.

18. The invention of Claim 17 wherein said fingerprint sensor is mounted on said second card.

19. The invention of Claim 16 wherein said fingerprint sensor and said transceiver are electrically connected to said system bus on the mounting of said first and said second cards in said expansion slot.

20. Apparatus for use in a system for secure identification comprising:
a wireless transceiver disposed on a first card;
a fingerprint sensor attached to said first card; and
a personal digital assistant having an expansion slot adapted to receive said card and thereby provide electrical communication between said sensor, said personal digital assistant and said transceiver.

21. The invention of Claim 20 wherein said personal digital assistant includes a central processing unit.

22. The invention of Claim 20 further including a system bus electrically connected to said personal digital assistant.

23. The invention of Claim 20 further including a second card adapted to electrically connect to said first card.

24. The invention of Claim 23 wherein said fingerprint sensor is mounted on said second card.

25. The invention of Claim 24 wherein said fingerprint sensor and said transceiver are electrically connected to said system bus on the mounting of said first and said second cards in said expansion slot.

26. Apparatus for use in a system for secure identification comprising:
first means for providing biometric data and
second means for transmitting said data via a wireless link.

27. The invention of Claim 26 wherein said second means is a wireless transceiver.

28. The invention of Claim 27 wherein said transceiver is a Bluetooth enable transceiver.

29. The invention of Claim 26 wherein said first means is a fingerprint sensor.

30. The invention of Claim 26 wherein said first and second means are operationally coupled to a Personal Digital Assistant.

31. A method for secure identification including the steps of:
providing biometric data and
transmitting said data via a wireless link.

32. The invention of Claim 31 wherein said step of transmitting further includes the step of transmitting said data via a Bluetooth enabled transceiver.

33. The invention of Claim 31 wherein said step of providing biometric data includes the step of providing biometric data via a fingerprint sensor.

34. The invention of Claim 31 wherein steps of providing said data and transmitting said data are executed via a Personal Digital Assistant.

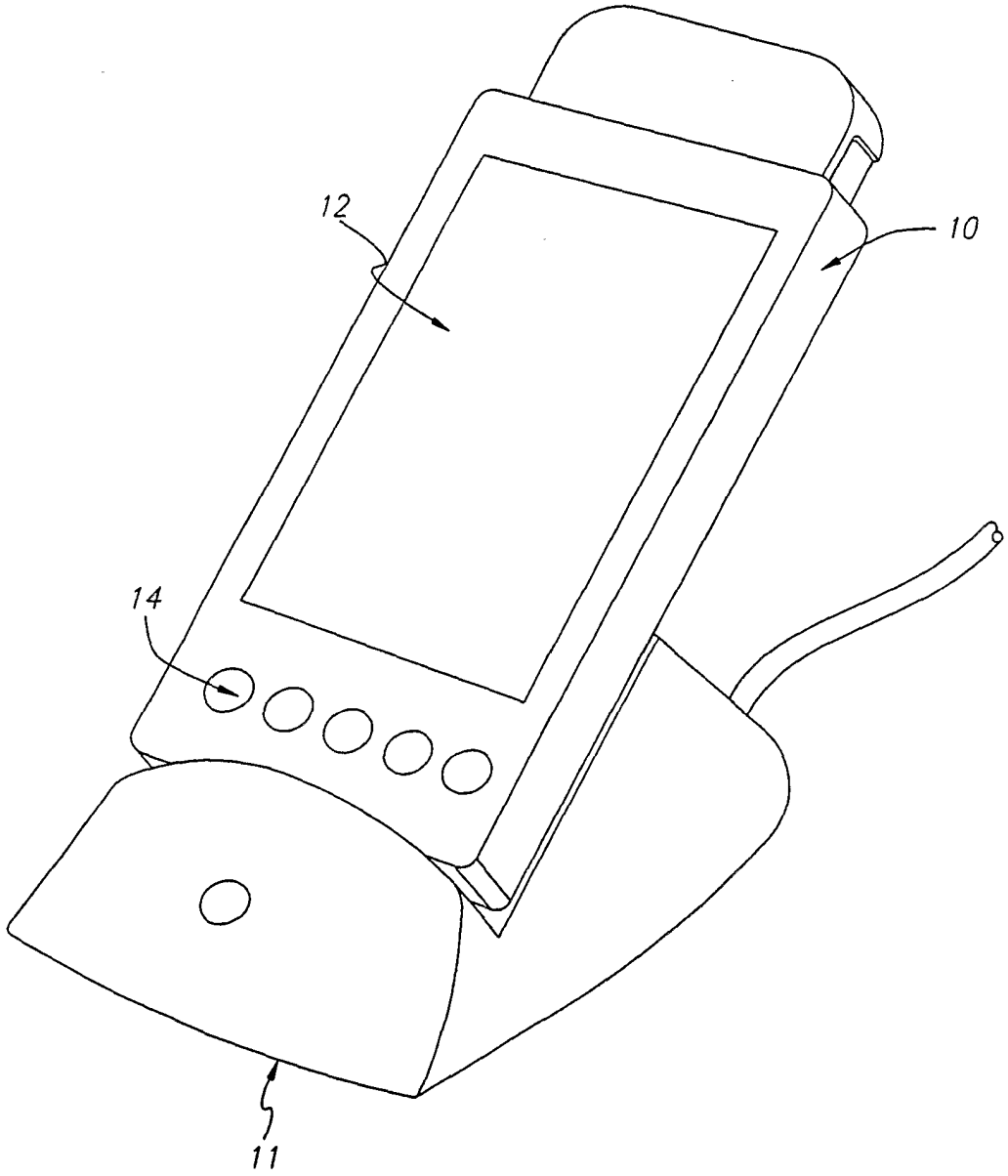

FIG. 1

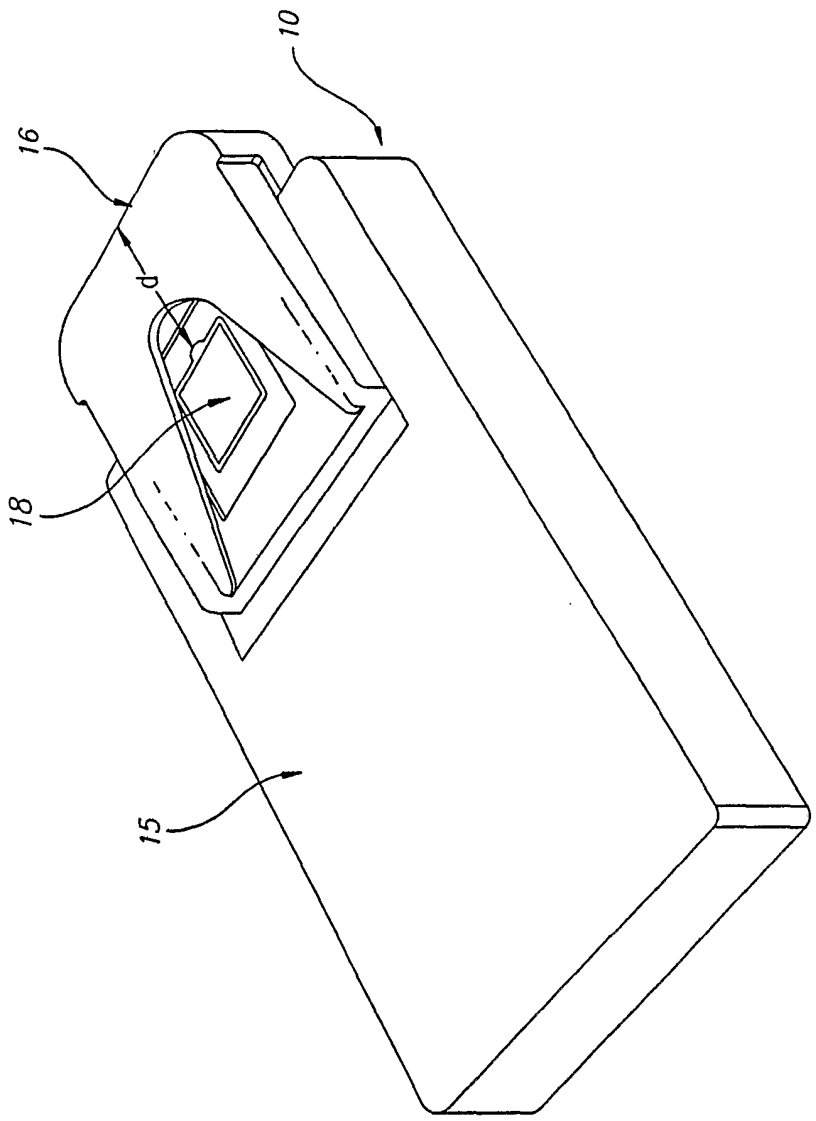

FIG. 2

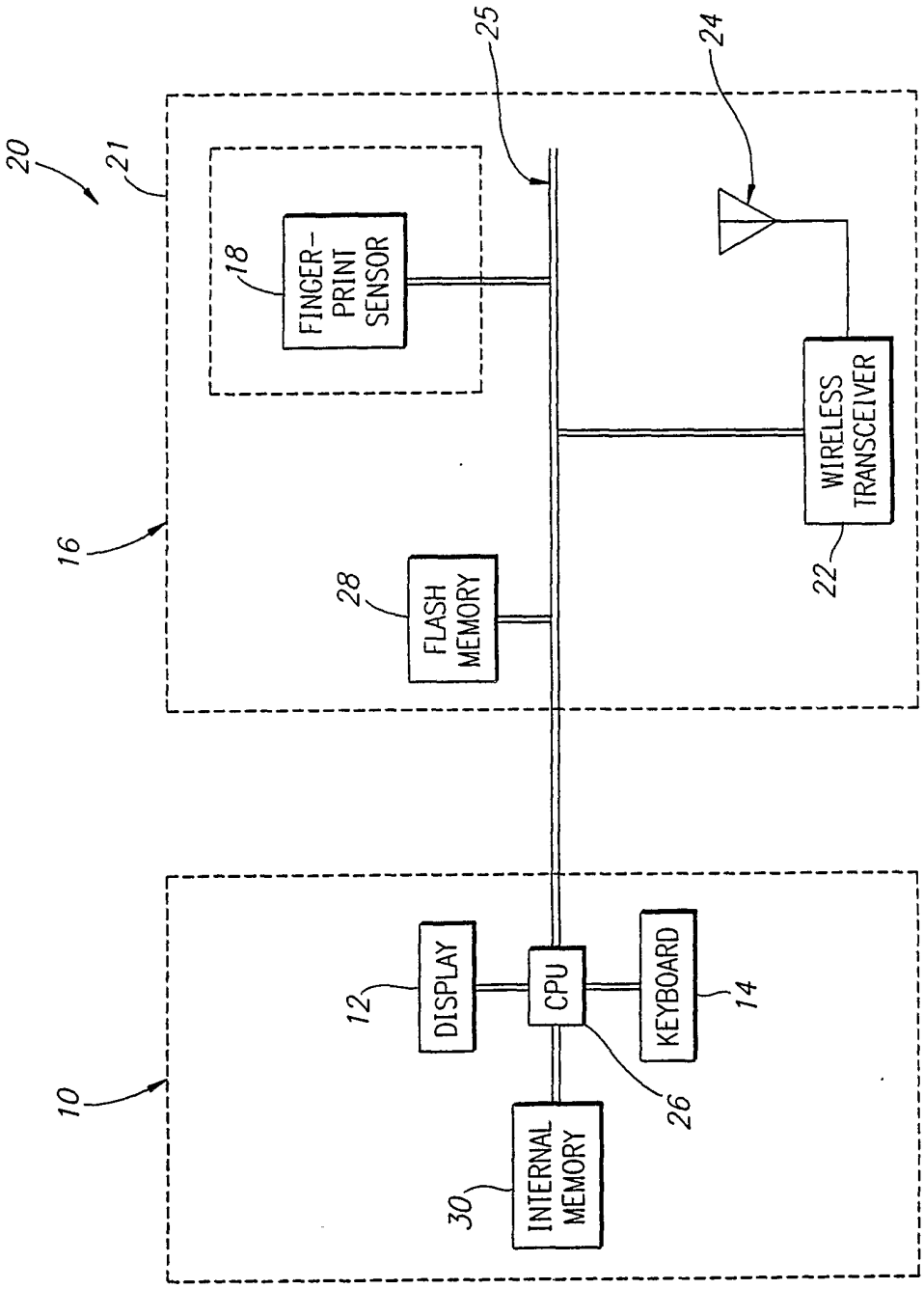
20
21
25
24
18
FINGER-PRINT SENSOR
WIRELESS TRANSCEIVER
16
22
28
FLASH MEMORY
12
DISPLAY
CPU
KEYBOARD
14
10
26
30
INTERNAL MEMORY

FIG. 3

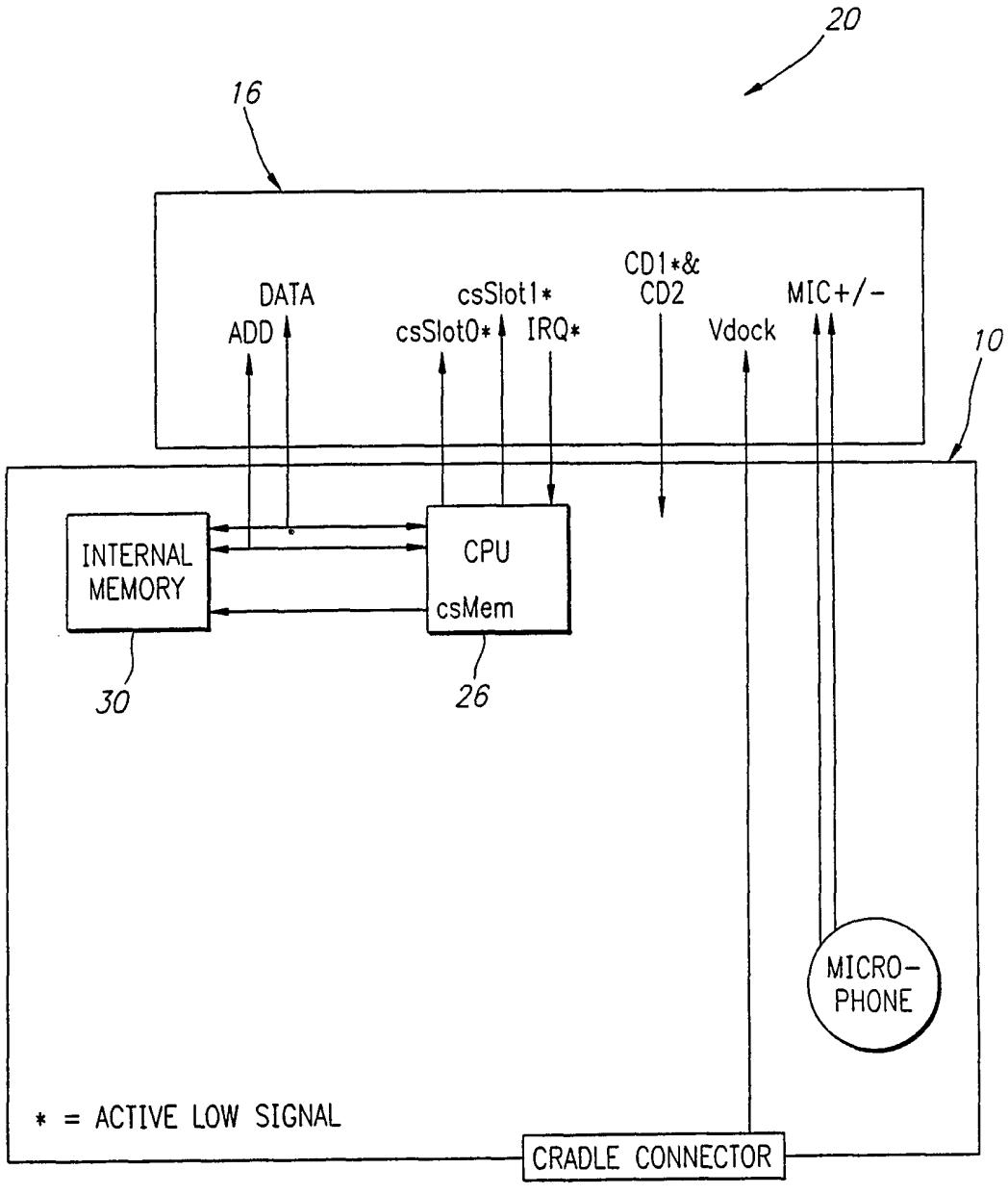
20
16
DATA
ADD
csSlot1*
csSlot0*
IRQ*
CD1*&
CD2
Vdock
MIC+/-
10
INTERNAL MEMORY
CPU
csMem
30
26
MICRO-PHONE
* = ACTIVE LOW SIGNAL
CRADLE CONNECTOR

FIG. 4

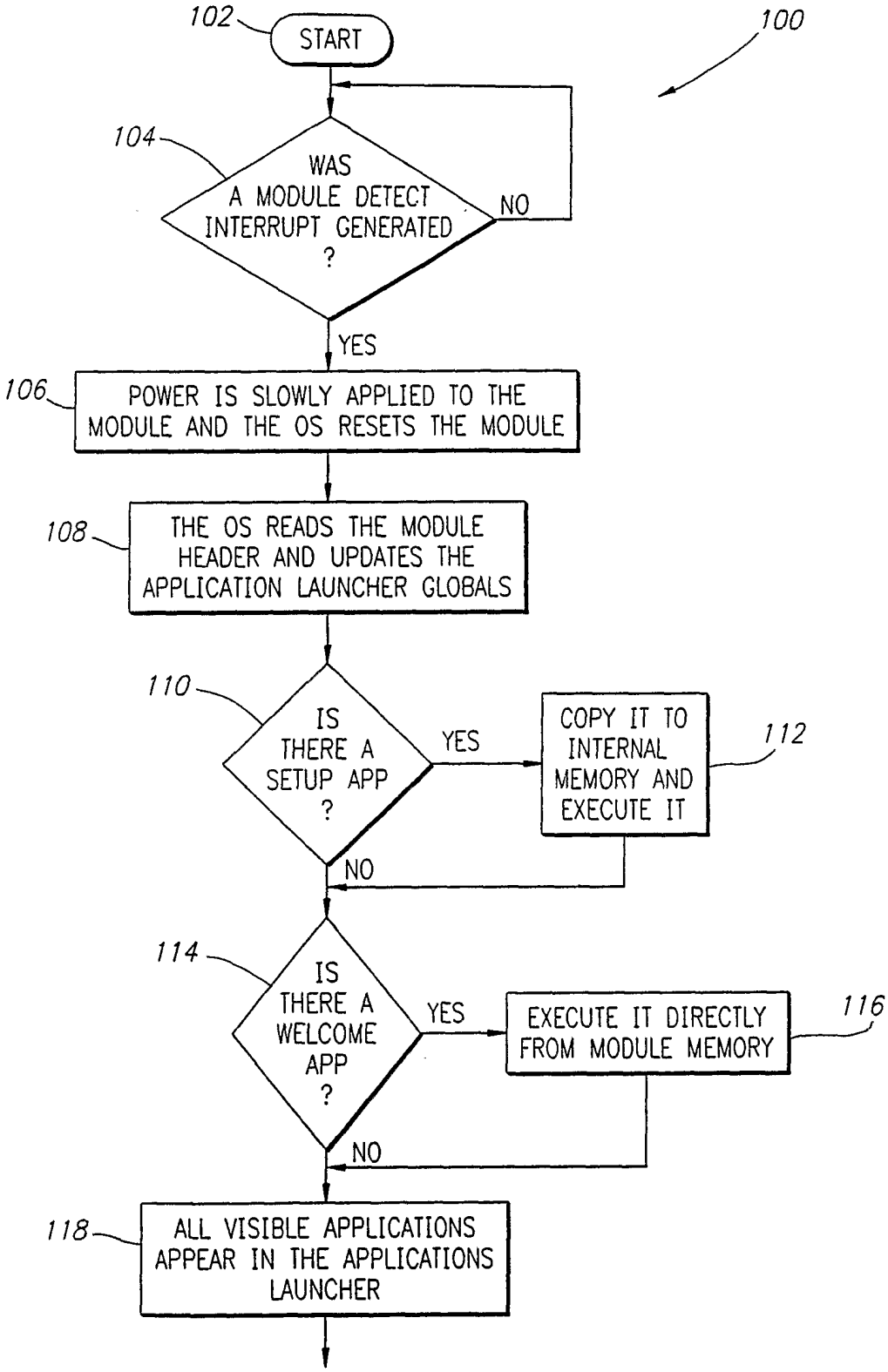
102
START
100
104
WAS A MODULE DETECT INTERRUPT GENERATED ?
NO
YES
106
POWER IS SLOWLY APPLIED TO THE MODULE AND THE OS RESETS THE MODULE
108
THE OS READS THE MODULE HEADER AND UPDATES THE APPLICATION LAUNCHER GLOBALS
110
IS THERE A SETUP APP ?
YES
COPY IT TO INTERNAL MEMORY AND EXECUTE IT
112
NO
114
IS THERE A WELCOME APP ?
YES
EXECUTE IT DIRECTLY FROM MODULE MEMORY
116
NO
118
ALL VISIBLE APPLICATIONS APPEAR IN THE APPLICATIONS LAUNCHER

FIG. 5(a)

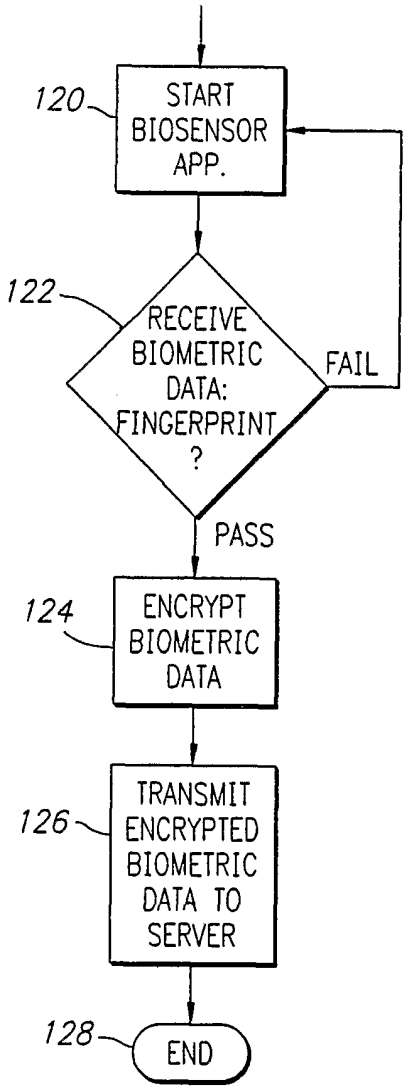
120
START BIOSENSOR APP.
122
RECEIVE BIOMETRIC DATA: FINGERPRINT ?
FAIL
PASS
124
ENCRYPT BIOMETRIC DATA
126
TRANSMIT ENCRYPTED BIOMETRIC DATA TO SERVER
128
END

FIG. 5(b)