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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 June 2002 (20.06.2002)

PCT

(10) International Publication Number
WO 02/49322 A2

(51) International Patent Classification[7]: H04M 1/00

(21) International Application Number: PCT/GB01/05492

(22) International Filing Date:
11 December 2001 (11.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0030183.8 11 December 2000 (11.12.2000) GB

(71) Applicant *(for all designated States except US)*: **CAMBRIDGE WIRELESS TECHNOLOGIES LIMITED** [GB/GB]; c/o Lakin Rose, Enterprise House, Vision Park, Cambridge CB4 4ZR (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HOLLOWAY, Paul** [GB/GB]; 19 Carlisle Close, Sandy, Bedfordshire SG19 1TY (GB). **FALCK, John** [GB/GB]; 36 New Barns Road, Ely, Cambs CB7 4PN (GB).

(74) Agent: **POWELL, Stephen, David**; Williams, Powell & Associates, 4 St. Paul's Churchyard, London EC4M 8AY (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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 02/49322 A2

(54) Title: MOBILE COMMUNICATION UNIT

(57) Abstract: A mobile telephone (10) includes a device (15) for checking the identity of a user in connection with various transactions. The device (15) may include one or more of fingerprint scanning means, voice or password recognition means (e.g. using a microphone of the telephone), photograph display means (e.g. using a display (12) of the telephone) or retina recognition means. The telephone also includes a short-range communication means (16, 17) for undertaking RFID smart card transactions. A user can load data representing money by means of a telephone communication into a memory (16) for use is subsequent transactions. Alternatively, current transactions may be validated. The memory (16) may have sub-divisions corresponding to different smart cards.

Mobile Communications Unit

The present invention relates to a mobile communication unit and more particularly to a unit with which a large variety of transactions can be undertaken.

Mobile telephones are growing ever more pervasive. Based on their increasing level of acceptance, it is predicted that within a few years most adults and many children will possess one. At the same time further development of the mobile telephone is taking place to enhance its functionality. For example the third generation (3G) telephone will include such additional features as the ability to receive digital broadcast, connection to the Internet and location information. It seems probable that the trend to include yet more functionality within the mobile telephone will continue. For example it would be advantageous to provide secure proximity operation using a mobile telephone.

For some time RFID smart cards have been used across a wide range of applications. These typically include mass transit, vending machines, access control and use as an electronic purse. RFID smart cards provide both a quick and convenient means for users to carry out such transactions. However RFID smart cards have a number of limitations that are of concern to users. The first of these is that in many applications no check is made by the system to verify that the user of the card is the true owner. A second limitation is that in order to replenish the card with money it must be inserted into a custom device which is located either at special cash points or in the user's home. A third objection is that users are irritated by the large number of cards that they are now obliged to carry.

When undertaking a transaction, such as a credit card payment by telephone, the parties have to rely on the customers giving their own card number. Thus problems of fraud and error arise. Uncertainty of customer identity also exists when making card payments in a store or making withdrawals from a cash machine. A further opportunity for fraud arises when making a purchase using the Internet connection on a WAP phone since no record of the Internet transaction exists.

The present invention seeks to overcome or reduce one or more of the above problems.

According to a first aspect of the present invention, there is provided a mobile communications unit comprising means for telephone communication connected to means for checking the identity of a user of the unit, so that the result of such a check can be incorporated in a telephone communication.

The check of identity may be associated with a transmission of information or with a transaction, e.g. a financial transaction.

The identity of a user is preferably checked biometrically, such as by voice recognition and/or by fingerprint scanning means. Alternatively, the identity check may be effected by means of a secret "PIN" number.

Preferably the means for telephonic communication includes a display, a microphone and a keypad and said means for checking identity is arranged to show a photograph of the user on said display, and/or incorporates means for recognising the voice of the user and/or a password spoken by the user when the user speaks into said microphone, and/or incorporates means for identifying a PIN number entered by a user on said keypad.

A positive result of a check may permit the user to undertake certain transactions telephonically, e.g. corresponding to a credit card payment or transferring a cash equivalent to a memory in the unit.

The unit may further include a relatively short-range communication means capable of undertaking transactions and the identity checking means may also be used to authorise such transactions.

The short-range communication means may include a device with a memory which is connected to receive and/or send data via the telephone communication means. The memory may be divided into a plurality of separate secure areas.

Alternatively, the short-range communications means may be part of a read/write module for communicating with a smart card located adjacent thereto.

According to a second aspect of the present invention there is provided a method of communicating between two telephone devices in which the identity of at least one of the parties is checked by the respective telephone device and the result of the check is sent via the telephone link to the other party.

In one embodiment there is provided a method of undertaking a transaction between two telephone devices comprising a first phase, in which details of the transaction are arranged via a telephone link, e.g. by voice or by data transfer, and a second phase, in which the identity of at least one of the parties is checked by the respective telephone device and the result of the check is sent via the telephone link to the other party.

Preferably one of the telephone devices incorporates a relatively short-range communication means and the method includes the step of undertaking a local communication using said communications means substantially simultaneously with, before or subsequent to a telephone communication.

Both of the telephone devices may incorporate data storage means with the method including the step of transferring data from the storage means of one of the telephone devices to the storage means of the other telephone device. The storage means may store data representing money.

One of the telephone devices may incorporate a read/write module with the method including the step of locating a smart card adjacent to said read/write module and the communication including the transfer of data to and/or from said smart card.

In order to implement preferred embodiments of the invention two additional modules are interfaced to the central processor unit of a mobile telephone. The first of these modules is an identification means. There are many methods available for providing secure verification of the user. All of them rely on data that is unique to the legitimate owner.

This can be either something that is known only to the user such as a PIN or a certain physical characteristic. Preferably a biometric method is used, since it provides a higher level of security than a PIN. There are already many suitable biometric techniques available that will analyse a particular human feature such as the retina, voice, fingerprint or vein. One preferred embodiment of the invention incorporates a fingerprint scanner. This is chosen because fingerprint devices are compact, well proven and accepted by the general public. An alternative preferred embodiment uses voice recognition combined with a pre-defined password as the verification means. This has the benefit that a microphone already exists as part of the mobile telephone leading to a saving in manufacturing cost.

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings of which:

Figure 1 shows a block diagram of a mobile telephone;

Figure 2 shows a modified telephone in communication with a nearby display system; and

Figure 3 shows another modified telephone for communication with a separate RFID card.

Referring to the drawing, a mobile telephone 10 comprises a central processor 11 connected to a display 12, a keypad or keyboard 13 and an antenna 14 for telephonic signals. A fingerprint scanner 15 is also connected to the central processor 11 and is physically mounted at the foot of the keypad 13. Also connected to processor 11 is an RFID (radio frequency identity) chip 16 corresponding to the chips found in RFID smart cards, or combi cards. The chip 16 is connected to an RFID antenna 17 which is tuned to 13.56 MHz by means of its inductance and the capacitance built into the input of the RFID chip 16.

The antenna 17 comprises a length of conductor configured as a coil around the perimeter of the telephone. The coil may be pre-fabricated on flexible sheet that is mounted on the

underside of the telephone. By using the largest possible surface area for the antenna, the operational range of the RFID element is maximised.

Thus it will be seen that two additional modules have been interfaced to the central processor unit of a conventional mobile telephone, viz a first module comprising a biometric reader in the form of a fingerprint scanner 15 and a second module comprising an antenna and a chip which is the same as that used in a conventional combi card. A combi chip typically has two external sets of inputs. The first input connects to the antenna as already described. The second input conventionally is connected to the pad on the combi card and provides a contact interface to its reader. When the user wishes to connect to an external host system the card is inserted into the contact reader. This enables the card to be connected for example to the user's bank account. In the present telephone, this second input is connected to the central processor 11. This permits the user for example to connect the combi chip to his bank account via his mobile telephone providing greater flexibility and convenience.

In order to understand better the concept of the invention, a typical cycle of activities carried out by the user during normal operation will be described.

On initial purchase of a mobile telephone, the new owner enrols his fingerprint. Each telephone is supplied with a unique access number that enables the learn mode of the fingerprint scanner. Once enabled the owner is requested to lay his finger on the scanner, which records his fingerprint. He is required to repeat this process a total of three times. Provided an acceptable match of the data is achieved, details of the owner's fingerprint are saved securely in the telephone. During the enrolment process it is possible as an option, to record a photograph of the owner. This is downloaded into a protected area in the memory of the central processor. Additionally, in order for the mobile telephone to provide the features of a credit card, the necessary bank details are securely entered into the memory of the chip 16.

It is possible also to enrol a number of secondary users on each mobile telephone. Secondary users are prevented from using the secure features of the telephone and only

have access to limited personal data. However, the feature allows other people to use the telephone in situations of need.

In order to operate the telephone, the owner must first switch on and then present his finger to the scanner. If the fingerprint is correctly verified all user functions in the telephone are enabled. The owner is now free to make normal telephone calls, connect to the Internet, use his telephone as a smart card or perform any other function that is provided. Failure to verify for any reason does not bar incoming calls. Emergency outgoing calls are also not barred.

In the event that the owner wishes to perform a transaction that involves a payment, it is first necessary to load the telephone with a sum of money. To do this the owner must connect his telephone to his bank account via the Internet. In order to log on to his bank account, the owner is asked initially to verify his identity using the fingerprint scanner 15. Once access is given to the bank account, the owner requests the transfer of a specific amount of money to his telephone. To complete the transaction, he again verifies his identity using the fingerprint scanner. The correct amount will then be transferred via the central processor of the telephone to the chip 16. Completion of the transfer will be confirmed on the display. At any time, the owner may request details of the amount of money present in the chip 16, which will be shown on the display 12.

Once the telephone has been loaded with money, the user is able to operate it for any payment application, just like with an RFID smart card. For example in a mass transit application, the user simply presents the telephone to the reader while passing through the gate or barrier. In doing so, the correct amount for the journey is automatically debited from the amount held in the owner's telephone.

The mobile telephone also provides a means to carry out normal day to day credit/debit purchases. On making a purchase, the owner of the mobile telephone presents it to a reader that is interfaced to the retailer's EPOS (electronic point-of-sale) system. Having verified that the user is the legal owner, the reader extracts the credit card details from the telephone. The amount to be paid will be entered by the sales assistant on the till. The two

pieces of information are combined and sent via the EPOS network to the user's bank. After deducting the amount of sale from the owner's account, details of the transaction are confirmed on the display 12. This takes the form of a message showing the name of the supplier, the amount that has been charged and the date of the transaction.

The user may also effect credit/debit processes completely telephonically, e.g. ordering and paying for theatre tickets from his home. Normal telephonic communication with the theatre is established, the transaction is arranged verbally or otherwise, the credit or debit card number is given, preferably automatically by the mobile telephone, and the transaction is confirmed by the user placing his finger on scanner 15, which supplies appropriate data signals to antenna 14 and thence to the theatre to approve and confirm the transaction. In this type of activity, the RFID antenna is not required.

Using these same principles there is almost no limit to the number of other possible applications for the purchase goods and services. For example the telephone could be presented to a reader fitted to a vending machine. After verification by the user, the vending machine will deduct the appropriate amount from the electronic purse in the telephone and dispense the product that had been requested. Similarly the telephone could be used as a means of making payments at restaurants. The customer would simply present his phone to the reader and enter the amount to be paid. Having verified the identity of the customer, the phone would complete the transaction with the customer's bank account. If required the reader would print a written receipt. In many restaurants the reader would be a portable unit connected to a base station via a radio LAN designed to 802.11 or use Bluetooth.

Ensuring that all financial transactions are logged through a trusted third party can provide an additional level of security. This operates as follows. Upon completion by the user of a purchase or cash transfer, the mobile phone automatically calls the trusted third party. Once contact is made, details of the transaction are passed to the trusted third party where they are logged in the user's account. If subsequently the user questions a transaction that he believes is shown incorrectly in his monthly bank statement, the user can produce the independent record of transactions held by the trusted third party as evidence.

The details of a limited number of financial transactions are retained within the telephone's FIFO memory and are available upon request on the display.

Where the owner is required to pay using current manual credit card procedures, it is possible for the owner to display his credit card number and expiry date on his telephone.

From time to time situations may exist where the user wishes to communicate over a distance by some means other than the mobile phone function. This can be achieved as shown in the modified phone 20 of Figure 2, by building additionally into the telephone either a radio LAN or a Bluetooth module 21. Using module 21 it is possible for the user to communicate with the outside world via a local base station 32 without incurring the cost of a mobile phone charge. Figure 2 shows such an arrangement in which a remote interactive display system 30 comprises a host computer 31, a base station in the form of receiver 32 and a monitor 33. This allows the user to operate the display 30 from the keypad on his phone. For example, at an airport the user could use the keypad to request specific details on a monitor 33 concerning flight information.

As an additional security measure the telephone includes an option to verify at regular intervals that the user of the telephone is the legitimate owner. The length of the interval between checks is defined when the telephone is in setup mode. In order to enter setup mode the owner first selects setup and then completes the process by verification on the fingerprint scanner.

A photograph of the legal owner stored within the mobile telephone may be used as an additional visual check of identity. Occasions arise in which authorities wish to verify the identity of a person. Typical examples are at passport control points, access to high security buildings or checks on the holders of driving licenses. To verify his identity, the legal owner simply presents his mobile telephone to a reader positioned at the control point while his finger is placed on the fingerprint scanner. Having processed details in the telephone about the owner, the reader transmits a command requesting the telephone to display the owner's photograph. This photograph may then be shown to the relevant

authority. The photograph will remain on the display for a predetermined period. This may be on display 12 or a separate display of the telephone 10.

The above-described arrangement has various advantages. In particular, it enables verification that the user of the mobile telephone is the legitimate owner. Once verification is complete the identity of the user subsequently may be checked either continuously or at predetermined intervals. Having established correct identity, the mobile telephone is enabled and the user is permitted access to the full range of features. One of these features is the ability of the mobile telephone to function as an RFID smart card. By presenting the telephone to a reader, the user is able to perform all conventional credit and debit card transactions. In addition the user is able very simply to transfer money from his bank account to his mobile telephone. It is necessary only to connect to his bank account via the Internet, request the amount and verify the transfer by means of the fingerprint scanner. The user can replenish his telephone from any point in the world where he is in radio contact.

The manufacturing cost of incorporating the fingerprint reader and RFID smart card functionality is low in relation to the overall cost of the telephone. In particular, fingerprint readers are already manufactured in high volume so that their cost is acceptable. In addition, they are compact, well proven and already generally accepted. Similarly chips for combi cards are also manufactured in high volumes and are therefore available at a relatively low price. By incorporating existing RFID technology, conformity to the ISO standards for proximity cards is ensured.

Various modifications can be made to the above-described arrangement. For example, the fingerprint scanner may be replaced or supplemented by other identity-checking means. Other possible biometric devices include means for identifying unique patterns in the user's eye, means for analysing the user's breath or saliva or blood (or other body fluid) or tissue. Alternatively, or in addition, voice recognition means may be employed, in which case the user can speak a password into the microphone which is incorporated in the unit. Alternatively, or in addition, photographic information and/or handwriting analysis means

may be employed. Alternatively, or in addition, the identity may be checked simply by the entry of a PIN number on keypad 13, although this technique is less secure.

If only telephonic communications are required, the RFID antenna 15 may be omitted, and the information stored in chip 16 may instead be stored in the memory within the mobile telephone 10.

If the only telephonic communications required are those from a fixed location such as the user's home or place of work, telephone 10 may be a non-mobile telephone.

For certain activities, both parties may be provided with a telephone 10 in accordance with the present invention. For example, to ensure that information is kept confidential, each party may reliably confirm his identity to the other before disclosure occurs. Of course, the information may be financially or commercially sensitive or be secret for other reasons.

Advantageously, the RFID smart telephone can be fully compatible with existing RFID cards. In the modification of Figure 3, an RFID reader/writer device 46 is incorporated in a mobile phone 40 and connected to central processor 11. Device 46 is connected to RFID antenna 47 which is in communication with a separate RFID card 45 having its own internal antenna (not shown). Provided card 45 is sufficiently near antenna 47, communications and transactions can be undertaken therewith. This arrangement enables the invention to be used with existing RFID cards. Another version of the telephone may incorporate a slot in which it is possible to insert a removable RFID combi card so that pads on the card conductively engage electrical conducts in the slot. The card is thus connected via its pads and the internal contacts of the telephone 10 to central processor 11. This arrangement allows an existing RFID combi card fully to replicate all of the features provided by RFID chip 16 and antenna 17.

There will also be situations where existing populations of user hold cards that are RFID only. The issuing authority may be reluctant for these users to exchange their cards for a version that is integrated within a mobile phone. Nevertheless it would still be possible for holders to perform transactions through a special version of the mobile phone. In this

instance the mobile phone would incorporate a read/write module. By laying the card against the phone a dialogue would take place between the two in the same way as if they were integrated within a single unit.

While it is envisaged that the telephone will be fitted with a chip conforming to the proximity card standard, this may not always be the case. The invention also covers the use of devices operating at frequencies other than 13.56 MHz. In addition devices capable of operating at greater ranges such as those defined in the ISO standard for vicinity cards may be incorporated.

The memory within the telephone 10 maybe sub-divided into a number of mutually secure areas partitioned by firewalls. This makes it possible to allocate service providers with individual areas for their particular application. As a consequence it becomes possible to incorporate the functionality of a number of different cards within the one mobile telephone. This is a real benefit to the user since he no longer has to carry in his wallet a collection of cards that he may rarely use. To satisfy the marketing aspirations of the different service providers, marketing information can be shown on the telephone's display 12 each time their service is used by the telephone owner.

The arrangement of Figure 2 may be further modified by omitting the RFID feature and/or the identity checking means 15 from mobile phone 20. The display system 30 can be replaced by any local interactive system.

CLAIMS

1. A mobile communications unit (10) comprising means (11-14) for telephonic communication connected to means (15) for checking the identity of a user of the unit so that the result of such a check can be incorporated in a telephone communication.

2. A unit according to claim 1, wherein the identity of a user is detected by biometric checking means (15).

3. A unit according to claim 1, wherein the identity of a user is detected by fingerprint scanning means (15).

4. A unit according to claim 1, wherein the means for telephonic communication includes a display (12), a microphone and a keypad (13) and said means (15) for checking identity is arranged to show a photograph of the user on said display (12), and/or incorporates means for recognising the voice of the user and/or a password spoken by the user when the user speaks into said microphone, and/or incorporates means for identifying a PIN number entered by a user on said keypad (13).

5. A unit according to any preceding claim and further including relatively short-range communication means (16, 17).

6. A unit according to claim 5, wherein said relatively short-range communication means includes a device (16) with a memory which is connected to receive and/or send data via the telephonic communication means (11-14).

7. A unit according to claim 6, wherein said memory is divided into a plurality of mutually secure areas.

8. A unit according to claim 5, wherein said relatively short-range communications means includes a read/write module (46) and an antenna (47) for communicating with a smart card located adjacent thereto.

9. A unit according to claim 5 wherein said relatively short-range communication means comprises a slot for receiving a smart card with contact pads, the slot including electrical contacts for conductively engaging the pads.

10. A method of communicating between two telephone devices in which the identity of at least one of the parties is checked by the respective telephone device (10) and the result of the check is sent via the telephone link to the other party.

11. A method according to claim 10, wherein the identity is checked biometrically.

12. A method according to claim 10, wherein the identity is checked by means of fingerprint scanning.

13. A method according to any of claims 10 to 12, wherein one of the telephone devices incorporates a relatively short-range communication means (16-17) and the method includes the step of undertaking a local communication using said communications means substantially simultaneously with, before or subsequent to a telephone communication.

14. A method according to any of claims 10 to 13, wherein both of the telephone devices incorporate data storage means and the method includes transferring data from the storage means of one of the telephone devices to the storage means of the other telephone device.

15. A method according to claim 14, wherein the storage means store data representing money.

16. A method according to any of claims 10 to 12, wherein one of the telephone devices incorporates a read/write module and the method includes the step of locating a smart card adjacent to said read/write module and the communication includes the transfer of data to and/or from said smart card.

17. A mobile communications unit (10) comprising means (11-14) for telephonic communication connected to a relatively short-range communication means (16, 17) including a device (16) with a memory which is connected to receive and/or send data via the telephone communication means.

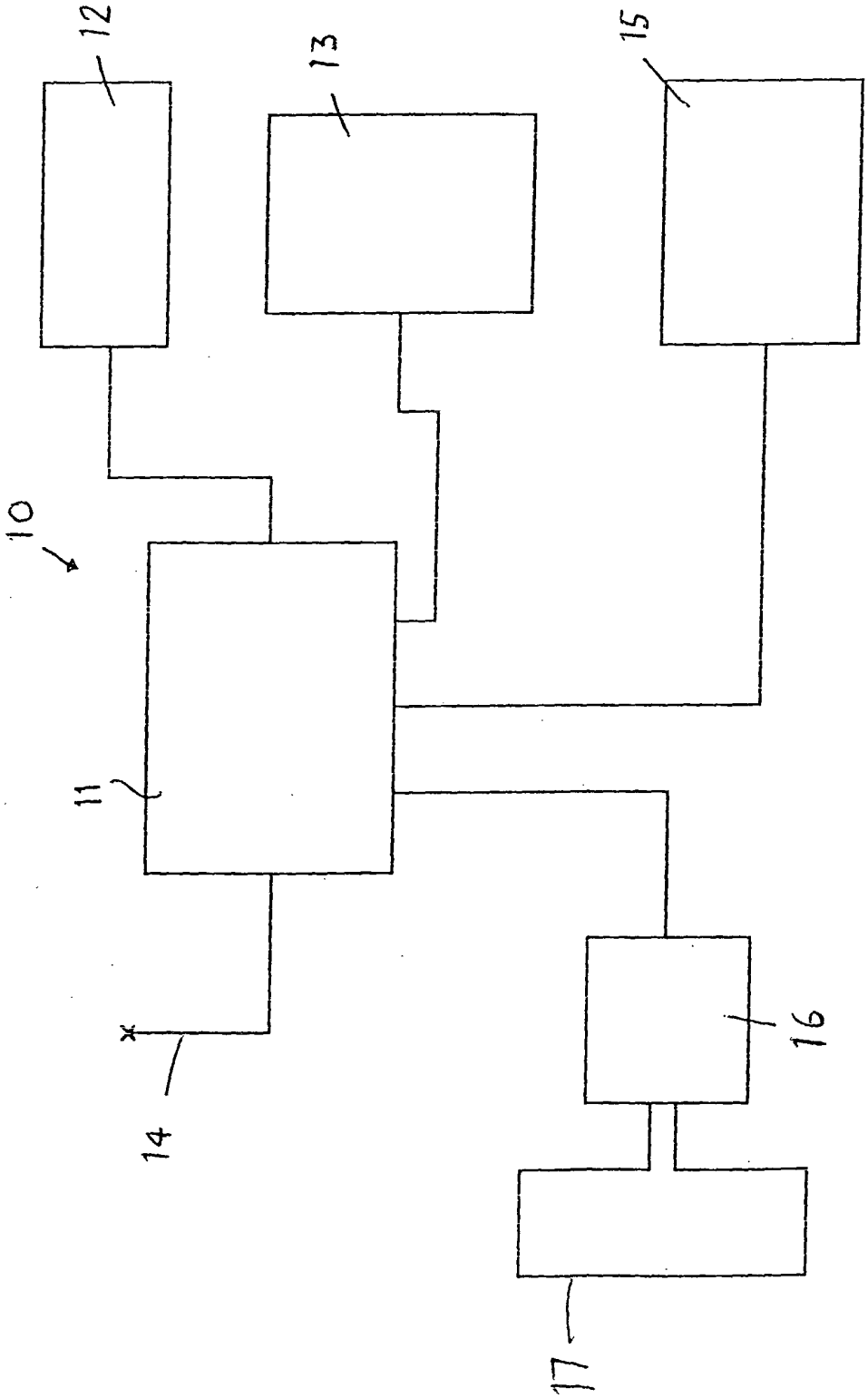

Fig 1

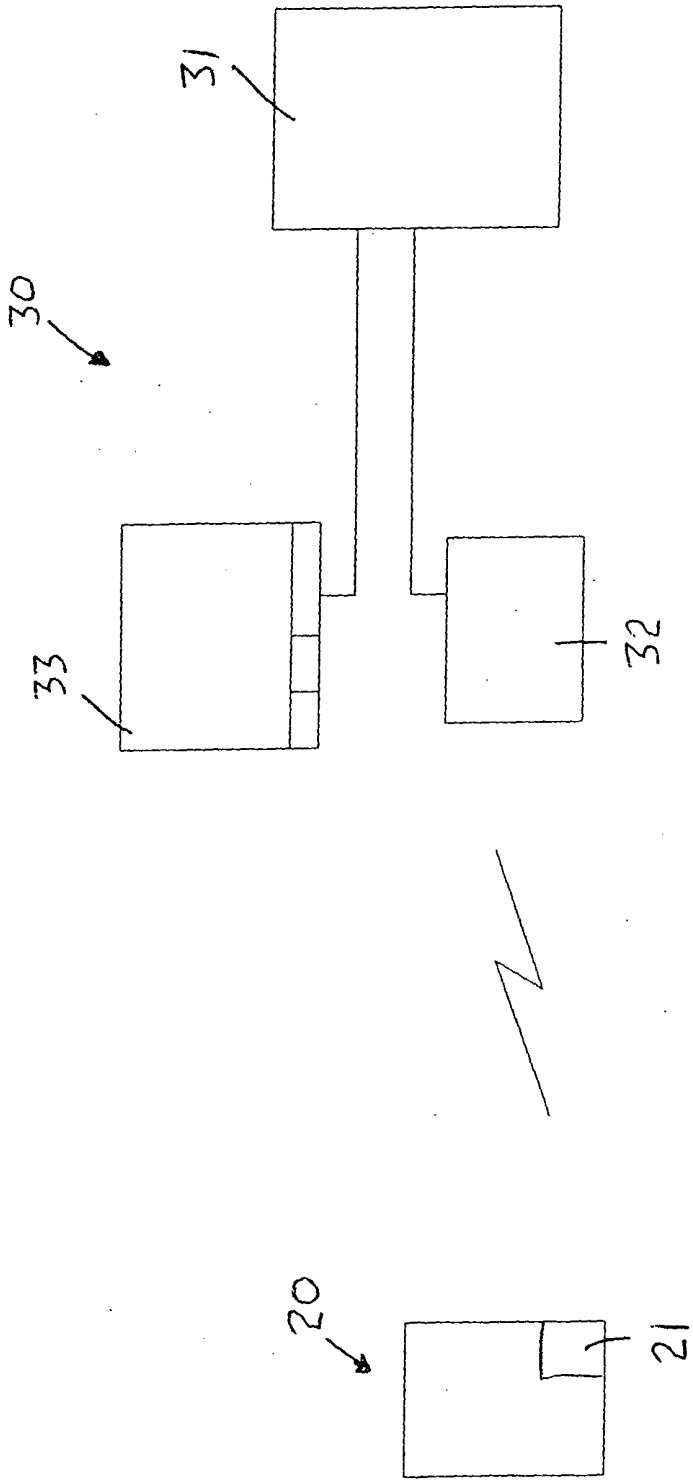

Fig 2

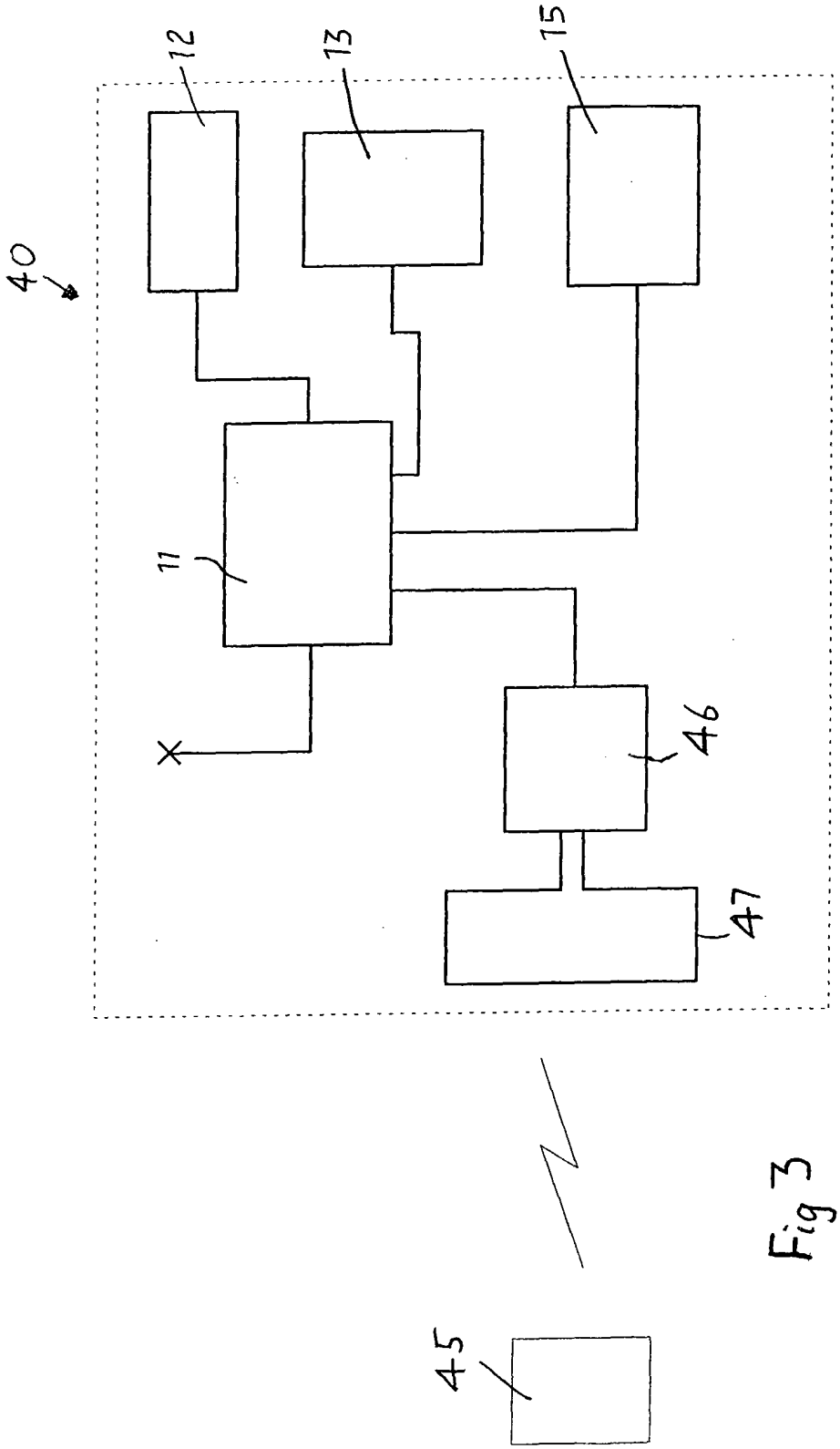

Fig 3

IPR2025-01237
Apple EX1032 Page 18