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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/089011 A1

(51) International Patent Classification⁷: H04Q 7/20

(21) International Application Number: PCT/US2004/009781

(22) International Filing Date: 26 March 2004 (26.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/458,314 28 March 2003 (28.03.2003) US

(71) Applicant (*for all designated States except US*): **WILDSEED, LTD.** [US/US]; 10210 NE Points Dr. Ste. 300, Kirkland, WA 98033 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **ENGSTROM, Eric, G.** [US/US]; 12415 Holmes Pt. Dr., NE, Kirkland, WA 98033 (US). **ZATLOUKAL, Peter** [US/US]; 218 Main Street, #480, Kirkland, WA 98033 (US).

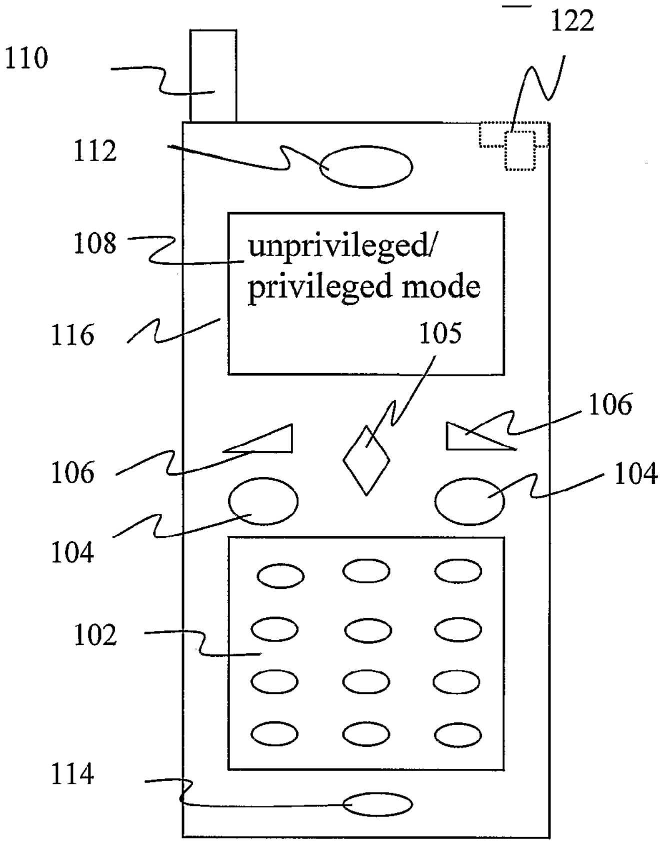
(74) Agents: **AUYEUNG, Aloysius, T., C.** et al.; Schwabe, Williamson & Wyatt, P.C., Pacwest Center, Suites 1600-1900, 1211 SW Fifth Avenue, Portland, OR 97204 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, 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, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH,

[Continued on next page]

(54) Title: A WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF OPERATION INCLUDING FINGER PRINT BASED AUTHENTICATION



(57) Abstract: A wireless mobile phone is equipped to operate in an unauthenticated and an authenticated mode of operation, depending on whether a user has been authenticated. In one embodiment, the wireless mobile phone includes a finger print reader to enable a user's finger print to be inputted and be used for authentication. In one embodiment, the finger print reader includes a light source and sensors, and having complementary logic to process emitted light reflected off a user's finger into an input finger print. The user is authenticated using the inputted finger print. In one embodiment, the finger print reader is integrated with a power on/off switch, which may be disposed on an end surface, a side surface or a front surface of the body of the phone.

GM, KE, LS, MW, MZ, 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, IT, LU, MC, 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).

Published:

— *with international search report*

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

A WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF OPERATION INCLUDING FINGER PRINT BASED AUTHENTICATION

RELATED APPLICATION

The present invention claims priority to provisional application number 60/458,314, filed March 28, 2003, entitled "A Wireless Mobile Phone With Authenticated Mode Of Operation Including Finger Print Based Authentication", and incorporated in its entirety by reference.

FIELD OF THE INVENTION

The present invention relates to the field of wireless mobile communication. More specifically, the present invention is related to, but not limited to, a wireless mobile phone having an authenticated mode of operation available only to an authenticated user, in particular, a user authenticated via the user's finger print.

BACKGROUND OF THE INVENTION

Advances in microprocessor and telecommunication technology have led to wide spread deployment and adoption of mobile devices, such as wireless mobile phones. For wireless mobile phones, in addition to wireless telephony, the late models are often equipped with advanced capabilities, such as calendar, address book, access to the World Wide Web (WWW), emails, and so forth.

Much of these functionalities are designed to increase the productivity of business users. As a result, it is not surprising that business users constitute a major user segment of wireless mobile phones, especially for the high-end function rich models. Increasingly, more business data, such as business contact information, business plans, sales/marketing strategies, financial reports, and so forth, are being stored on wireless mobile phones.

However, unlike personal computers or other computing devices, where user authentication, through e.g. user log-in, are routinely provided with virtually all operating systems, few if any operating systems of wireless mobile phones provide means to authenticate users. As a result, under the prior art, wireless mobile phones are at risk of unauthorized usage, as well as data being compromised by unauthorized accesses.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates a front view of a wireless mobile phone incorporated with the teachings of the present invention, in accordance with one embodiment;

Figures 2a-2b illustrate a top view and a side view of the power switch of **Fig. 1**, having an integrated finger print reader, in accordance with one embodiment;

Figures 3a-3b illustrate two architectural views of the wireless mobile phone of **Fig. 1**, in accordance with one embodiment;

Figures 4a-4b illustrate the operational flow of the relevant aspects of the operating logic of **Fig. 3b**, in accordance with one embodiment;

Figure 5 illustrates a front view of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with an alternate embodiment;

Figures 6a-6b illustrate two perspective views of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with yet another embodiment;

Figures 7a-7b illustrate a front view and a side view of another wireless mobile incorporated with another aspect of the teachings of the present invention, in accordance with yet another embodiment; and

Figures 8a-8b illustrate a front view and a back view of the identity card of **Fig. 7b** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Embodiments of the present invention includes but not limited to a wireless mobile phone having an authenticated mode of operation, available only to an authenticated user, in particular, a user authenticated by the user's finger print.

Parts of the description will be presented in terms commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. The term "wireless mobile phone" as used herein (in the specification and in the claims) refers to the class of telephone devices equipped to enable a user to make and receive calls wirelessly, notwithstanding the user's movement, as long as the user is within the communication reach of a service or base station of a wireless network service provider. Unless specifically excluded, the term "wireless mobile phone" is to include the analog subclass as well as the digital subclass (of all signaling protocols).

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation.

The phrase "in one embodiment" is used repeatedly. The phrase generally does not refer to the same embodiment, however, it may. The terms "comprising", "having" and "including" are synonymous, unless the context dictates otherwise.

Referring now to **Figures 1** and **3a-3b**, wherein a front view and two architecture (internal component) views of a wireless mobile phone of the present invention, in accordance with one embodiment, are shown. As illustrated, wireless mobile phone **100** of the present invention (hereinafter, simply phone **100**) is advantageously provided with operating logic **240** equipped in particular with security function **242**, to operate phone **100** in at least an unauthenticated mode of operation and an authenticated mode of operation.

While operating in the unauthenticated mode of operation, i.e. without having the user authenticated, operating logic **240** makes available only a limited or reduced set of functions, whereas under the authenticated mode of operation, i.e. having the user authenticated, operating logic **240** makes available a more expanded or the entire set of functions.

The exact constitution of the limited/reduced set of functions and the expanded/full set of functions is application dependent, which may vary from embodiments to embodiments. In one embodiment, the limited/reduced set of functions include only the ability to make an emergency call, such as a 911 call, otherwise, no other functions, including but not limited to making other calls, accessing calendar, email, text messaging, viewing and/or storing documents, and so forth, are permitted. These other functions are available only under the authenticated mode.

In another embodiment, the limited/reduced set of functions may effectively be a null function set, excluding even the ability to make an emergency call, except for notification of the unauthenticated status of the user, and perhaps, inviting the user to authenticate himself/herself, by e.g. providing a finger print input.

In various embodiments, in addition to the above described unauthenticated and authenticated modes of operation, operating logic **240** further supports a provisioning mode of operation, under which phone **100** is initially provisioned. Under the initial provisioning mode, conventional provisioning, such as configuring phone **100** for a particular wireless carrier, a particular subscriber and so forth, may be performed. Entry into the initial provisioning mode may be effectuated in any one of a number of conventional approaches.

Continue to refer to **Figures 1** and **3a-3b**, for the illustrated embodiment, phone **100** is further advantageously equipped with finger print reader **232** to facilitate a user to input his/her finger print, and security function **242** is equipped to authenticate the user by the user's inputted finger print. In other words, operating logic **240** operates phone **100** in the authenticated mode, and makes available the expanded/full set of functionalities, only if the user has been authenticated by his/her finger print, otherwise, phone **100** is operated in the unauthenticated mode with only a limited/reduced set of functionalities (except in the initial provisioning mode).

For the embodiment, operating logic **240**, more specifically, security function **242**, also supports the provision of a finger print, and its saving in the form of an image, for use as a reference to authenticate an inputted finger print for authentication of a user, and operation of phone **100** in the authenticated mode. In various embodiments, the saving of the reference finger print image is also supported under a special configuration mode, while operating in the authenticated mode. Entry into the configuration mode (while operating in the authenticated mode) may also be effectuated in any one of a number of conventional means.

Further, for the illustrated embodiment, finger print reader **232** is advantageously integrated with power on/off button **122**, to enable a user's finger print to be inputted seamlessly as part of the power-on process.

Moreover, for the illustrated embodiment, power on/off button **122** (integrated with finger print reader **232**) is disposed at the top end surface of body **116** of phone **100**. As will be described in more detail below, referencing **Figs. 5** and **6a-6b** in particular, power on/off button **122** (integrated with finger print reader **232**) may be disposed on other surfaces of the body of a wireless mobile phone.

Referring now also to **Figures 2a-2b**, wherein a top view and a side view of power on/off button **122** with integrated finger print reader **232** is illustrated in further detail, in accordance with one embodiment. As illustrated, for the embodiment, power on/off button **122** includes transparent body **124** (which transparency is represented by the hash lines) having flanges **126**, which undersides include contacts **142**. Contacts **142** are employed to close/open switch circuit **228**, as power on/off button **122** is moved from a rest position to a depressed position. When closed, switch circuit **228** allows power from power supply **222** to be provided to from finger print reader **232** and other components **202-212** of phone **100**. When open, switch circuit **228** cutoffs power of power supply from finger print reader **232** and other components **202-212** of phone **100**. Power on/off button **122** also includes a counterforce exerting means (not shown), such as a spring like assembly, to exert a counterforce to restore power on/off position **122** from the depressed position to its rest position.

For the embodiment, finger print reader **232** includes light source **234** and sensors **236**. Light source **234** is employed to emit light, and sensors **236** are employed to sense the emitted light (passing through transparent body **124** of power on/off button **122**) and reflected off finger **150** of the user (back through transparent body **124** of power on/off button **122**). In one embodiment, light source **234** comprises one or more light emitting diodes (LED), and sensors **236** comprise an array of micro photo sensors.

Sensors **236** output signals responsive to the reflected light sensed. The signals in turn are processed by DSP **204** into an image, more specifically, an input finger print image. Security function **242**, executed by processor **202**, in turn compares the input finger print image against the reference finger print image to authenticate the user.

In alternate embodiments, non-optical finger print readers, such as capacitance based finger printer readers may be employed instead. For these embodiments, sensors **236** output signals responsive to the electrical interactions between the embedded capacitors and the user's finger, which vary according to the print contour. The signals output by sensors **236** may be processed into a finger print data structure and/or image. In yet other embodiments, other non-capacitance based, non-optical finger print readers may be employed instead.

Referring again to **Fig. 1** and **3a-3b**, additionally, phone **100** includes conventional wireless telephony elements, including audio communication elements, such as ear speaker **112** and microphone **114**, and non-audio communication elements, such as input key pad **102** having a number of alphanumeric input keys and display **108**. Further, the non-audio input elements may further include scroll button **105**, selection buttons **106**, and "talk" and "end talk" buttons **104**. These elements are disposed on various external surfaces of body **116**.

Externally, phone **100** may also include antenna **110**. Keys of key pad **102** may be surrounded by, or otherwise include illuminable light emitting diodes (LED) in their backgrounds. For the purpose of the present specification, the terms "button" and "key" may be considered synonymous, unless the context clearly indicates otherwise.

Internally, in addition to processor **202** and DSP **204**, phone **100** also includes non-volatile memory **206**, general purpose input/output (GPIO) interface **208**, and transmit/receive (TX/RX) **212**, coupled to each other, processor **202** and DSP **204**, via bus **214**, and disposed on a circuit board **220**.

Except for novel manner that many of these elements, such as processor **202**, DSP **204** and so forth, are used in support of making the expanded/full set of functionalities available only to an authenticated user, the enumerated elements otherwise perform their conventional functions known in the art.

Non-volatile memory **206** is employed to store programming instructions and optionally, working data, including operating logic **240** and its security function **242**. Working data may include callee/messaging party or parties (e.g. their phone numbers or IP addresses) with whom user may communicate. Working data may include the reference and input finger print images of the user.

Processor **202**, assisted by DSP **204**, is employed to operate phone **100**, executing operating logic **240**, including security function **242**.

Keys of key pad **102** may be employed to enter alphanumeric data, including entering a sequence of alphanumeric data for the phone number or address of a "callee". Selected sequence of the keys (such as "*#") may also be employed to denote a user instruction to return to the unauthenticated mode of operation, if entered while operating in the authenticated mode of operation, or to return to the authenticated mode of operation, if entered while operating in the unauthenticated mode of operation (provided the user is authenticated).

Scroll key **105** and companion selection keys **106** may be employed to scroll and select various options or list items of various menu options or selection lists, including scrolling and selecting list items presented for user interactions to verify the user's wellness. For the embodiment, scroll key **105** may be selected in one of two positions, an "up" position or a "down" position for scrolling a selection list in an "up" direction and a "down" direction respectively. Similarly, scroll and selection keys **105/106** may also be employed to select a menu item to convey a user instruction to return to the unauthenticated mode, if the selection is made while operating in the authenticated mode, or to return to the authenticated mode, if the selection is made while operating in the unauthenticated mode (provided the user is authenticated).

GPIO **208** may be employed to generate input signals, such as a corresponding "alphanumeric" signal in response to a user selection of one of the keys of key pad **102**, a "scroll" signal" (or more specifically, a "scroll up" or a "scroll down" signals) in response to a user selection of scroll key **105**, a "selection" signal in response to a user selection of select button **106**, and so forth.

TX/RX **212** may be employed to transmit and receive communication signals for a call and/or a text message. TX/RX **212** may be a radio frequency transceiver, and support one or more of any of the known signaling protocols, including but are not limited to CDMA, TDMA, GSM, and so forth.

The constitutions of these elements are known, and will not be further described.

As to operating logic **240**, including security function **242**, it may be implemented in the assembly or machine instructions of processor **202**, or a high level language that can be compiled into these assembly or machine languages.

Accordingly, except for the enhancements provided, phone **100** otherwise represents a broad range of wireless mobile phones, including both the analog as well as the digital types (of all signaling protocols), substantially rectangular uni-body as illustrated, or curved uni-body, as well as multi-portions, such as "flip phones" to be illustrated later.

Figure 4 illustrates the operational flow of the relevant aspects of operating logic **240**, in accordance with one embodiment. As illustrated, on start up/reset (such as depression of power on/off button **122** by a user), operating logic **240** enables phone **100** to operate in the earlier described unauthenticated mode, making available only a limited/reduced set of functionalities, block **402**. Thereafter, operating logic **240** waits for additional user input, block **404**.

Recall from earlier description, on closure of switch circuit **228**, power is provided to finger print reader **232** and other components **102-212** of phone **100**. Thus, if a user continues to keep his/her finger on power on/off switch, even after closing switch circuit **228** and powering on phone **100**, integrated finger print reader **232**, supported by DSP **204**, enables a finger print image to be seamlessly inputted for user authentication.

Accordingly, on receipt of inputs, operating logic **240** determines if the input is finger print input provided via finger print reader **232**, block **406**. In various embodiments, processor **202** may be notified (e.g. interrupted) by DSP **204** upon completion by DSP **204** in generating an input finger image.

If the user input is a finger print image, operating logic **240** (or more specifically, security function **242**) determines if phone **100** is operating in the unauthenticated mode, within the configuration mode of the authenticated mode, or the initial provisioning mode, block **407**.

If phone **100** is determined to be operating in either, the configuration mode within the authenticated mode, or the initial provisioning mode, operating logic **240** (or more specifically, security function **242**) saves the inputted finger print image as a reference finger print image, block **408**.

If phone **100** is determined to be operating in the unauthenticated mode, operating logic **240** (or more specifically, security function **242**) initiates the finger print based authentication process, authenticating the user by comparing the received input finger print image, against the previously saved reference finger print image, block **409**.

If the inputted finger print image does not substantially match the previously saved reference finger print image, block **410**, operating logic **240** (or more specifically, security function **242**) reports the authentication failure, block **412**, and continues to operate phone **100** in the unauthenticated mode at block **404**.

However, if the inputted finger print image substantially matches the previously saved reference finger print image, block **410**, operating logic **240** (or more specifically, security function **242**) enables phone **100** to operate in the authenticated mode, block **414**. Thereafter, operating logic **240** continues operation at block **404**.

The precision level at which an inputted finger print image is to be considered substantially matching with a reference finger print image is application dependent. Preferably, different user selectable precision levels are offered. As with other user selectable options, the selection may be facilitated in any one of a number of known user selection techniques.

Back at block **408**, if the input is determined not to be finger print input, operating logic **240** determines if the input is a user instruction to return to the unauthenticated mode of operation (e.g. a user selecting or inputting such command using alphanumeric keys **102** and/or scroll/select keys **105** and **106** while operating in an authenticated mode of operation), block **416**.

If the input is determined to be a user instruction to return to the unauthenticated mode of operation, operating logic **240** (or more specifically, security function **242**) returns phone **100** to operate in the unauthenticated mode, block **418**. Thereafter, operating logic **240** continues operation at block **404**.

In one embodiment, before exiting to the unauthenticated mode, operating logic **240** (or more specifically, security function **242**) causes a user selectable "resume" (i.e. re-authentication) option to be rendered on display **108**. Selection of the option is processed as if phone **100** is being powered on or reset. That is, operating logic **240** causes a finger print of the user to be read and inputted.

If the input is determined to be other user inputs, operating logic **240** handles the other user inputs in an application dependent manner, block **420**. In particular, if the input is a user instruction to return to the authenticated mode of operation, operating logic **240** continues operation at block **404**, and awaits for finger print input. If the input is other conventional inputs, the inputs are processed as in the prior art. Thereafter, operating logic **240** continues operation at block **404**.

Figure 5 illustrates another embodiment of the wireless mobile phone of the present invention. More specifically, **Fig. 5** illustrates a front view of the alternate embodiment. The alternate embodiment is substantially that of the embodiment of **Fig. 1**, except that phone **100** is substantially rectangular in shape, whereas phone **500** has a curved shape. Also, power on-off button **522** with integrated finger print reader is disposed at a side surface of body **516** of phone **500** instead.

Figures 6a-6b illustrate yet another embodiment of the wireless mobile phone of the present invention. More specifically, **Fig. 6a-6b** illustrate two perspective views of the embodiment. The embodiment is also substantially that of the embodiments of **Figs. 1** and **5**, except that phone **100** is substantially rectangular, phone **500** has a curve shaped body, whereas phone **700** has a multi-section body.

The multi-section form factor includes a first section **716b** and a second section **716c**, and the second section **716c** is further comprised of at least two sub-sections **716d-716e**. The first and second sections **716b-716c** may pivot towards each other as denoted by direction arrow **706a** or away from each other opposite to the direction denoted by arrow **706a**. Sub-section **716d** may rotate relative to sub-section **716e** as denoted by the directions denoted by arrows **706b**. In other words, phone **700** may be considered as an improved version of what is commonly referred to as "flip" phones.

Similar to the earlier described embodiments, phone **700** is provided with operating logic having a security function as earlier described, and power on/off button **722** with an integrated finger print reader. Except, power on/off button **722** with the integrated finger print reader is disposed at a front surface of lower section **716c** of phone **700** instead.

In alternate embodiments, second section **716c** may be a uni-section, i.e. it is not further sub-divided into to relatively pivotable sub-sections.

In yet other embodiments, the reference figure print image may be provided to the wireless mobile phone in a secure manner, e.g. read from an identity card, via an identity card reader additionally provided to the wireless mobile phone.

Figures 7a-7b illustrate one such embodiment. As illustrated in **Fig. 7b**, wireless mobile phone **100** is additional endowed with an identity card reader **740**. Identity card reader **740** (optionally, assisted by a device driver additionally provided to supplement operating logic **240**) is equipped to retrieve the earlier described reference finger print image from identity card **742**.

Preferably, identify card **742** has a form factor that is difficult to forge, and its issuance is governed by a secured process. Resultantly, security for wireless mobile phone **100** is further enhanced.

For the embodiment, identity card **742** comprises a smart electronic card **744** (commonly referred to as a smart card) (see **Fig. 8a-8b**), and the reference finger print image is pre-stored in the embedded smart card **744**. Operating logic **240** (optionally, supplemented by a corresponding reader device driver) retrieves the reference finger print image from embedded smart card **744**, on detection of the presence of identity card **742**.

In various embodiments, the reference finger print image may be further protected via encryption, requiring operating logic **240** to posses the proper decryption key to recover the reference finger print image after retrieval.

In yet other embodiments, the reference finger print image may be further protected via an authentication protocol, requiring wireless mobile phone **100** to be equipped with the appropriate credential to authenticate itself to smart card **744**, before being allowed by smart card **744** to access the pre-stored reference finger print image in smart card **744**.

In yet other embodiments, the reference finger print image may be imprinted on identity card **742**, and identity card reader **720** is an optical reader.

In yet still other embodiments, the reference finger print image may be encoded via a magnetic strip disposed on a surface of identity card **742**, and identity card reader **720** is a magnetic code reader.

These are just a few example, other equivalent encoding/storing and reading/retrieving techniques may also be employed instead.

Conclusion and Epilogue

Thus, it can be seen from the above descriptions, a novel wireless mobile phone that can afford protection against unauthorized access to user data and/or usage of the phone has been described.

While the present invention has been described in terms of the foregoing embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims.

In particular, the present invention may be practiced with the finger print reader (optical or otherwise) not being integrated with power on/off button, as well as employing additional and/or other means to authenticate a user.

Thus, the description is to be regarded as illustrative instead of restrictive on the present invention.

CLAIMS

What is claimed is:

1. A wireless mobile phone comprising:

a plurality of components coupled to each other to facilitate wireless telephony communication by a user;

an input mechanism to facilitate input of a finger print of the user; and

operating logic to receive input from the input mechanism and to selectively operate the components depending on whether the user is successfully authenticated via an inputted finger print.

2. The wireless mobile phone of claim 1, wherein said input mechanism comprises a light source to emit light, and an array of light sensors to sense the emitted light reflecting off a user's finger.

3. The wireless mobile phone of claim 2, wherein the wireless mobile phone further comprises processing logic associated with the input mechanism to process the reflected light sensed into an input finger print.

4. The wireless mobile phone of claim 3, wherein the operating logic further comprises logic to compare the input finger print against a reference finger print.

5. The wireless mobile phone of claim 1, wherein the wireless mobile phone further comprises a reader to facilitate provision of a reference finger print via an identity card.

6. The wireless mobile phone of claim 5, wherein the reference finger print is stored on said identity card in a manner to be read by a reader selected from the reader group consisting of an electronic reader, an optical reader, and a magnetic reader, and the reader is a corresponding selected one of the electronic reader, the optical reader and the magnetic reader.

7. The wireless mobile phone of claim 6, wherein said input mechanism comprises one or more capacitors, and one or more sensors coupled to the one or more capacitors to sense electrical interaction with the capacitors by a user's finger, and to output signals indicating of the user's finger print.

8. The wireless mobile phone of claim 7, further comprising processing logic associated with the input mechanism to process the reflected light sensed into an input finger print.

9. In a wireless mobile phone, a method of operation comprising:

receiving finger print input from a user;

authenticating the user using the provided finger print input; and

operating a plurality of components of the wireless mobile phone to facilitate wireless telephony communication by the user, depending on whether the user was successfully authenticated via the received finger print input of the user.

10. The method of claim 9, wherein said receiving of finger print input from the user comprises emitting light using a light source, sensing the emitted light reflecting off the user's finger using a plurality of sensors, and processing the reflected light sensed into a finger print input.

11. The method of claim 10, wherein the method further comprises comparing the inputted finger print against a reference finger print.

12. The method of claim 11, wherein the method further comprises retrieving the reference finger print from an identity card.

13. The method of claim 9, wherein said receiving of finger print input from the user comprises sensing electrical interactions with one or more capacitors by the user's finger using a plurality of sensors, and processing the sensed interactions into an inputted finger print.

14. A wireless mobile phone comprising:

a plurality of components coupled to each other to facilitate wireless telephony communication by a user, with the components being equipped to operate in at least a selected one of a first mode and a second mode; and

operating logic to operate the components in said first mode without authentication of the user, and to operate the components in said second mode if the user is successfully authenticated.

15. The wireless mobile phone of claim 14, wherein the operating logic enables the components to provide first one or more functions while operating the components in said first mode, and further enables the components to provide second additional one or more functions, while operating the components in said second mode.

16. In a wireless mobile phone, a method of operation comprising:

operating a plurality of components coupled to each other to facilitate wireless telephony communication by a user, in a first mode, prior to authenticating the user;

receiving input for authenticating the user; and

operating the components in a second mode if the user is successfully authenticated.

17. The method of claim 16, wherein said operating of the plurality of components in said first mode comprises enabling the components to provide first one or more functions, and said operating of the plurality of components in said second mode comprises enabling the components to further provide second one or more functions.

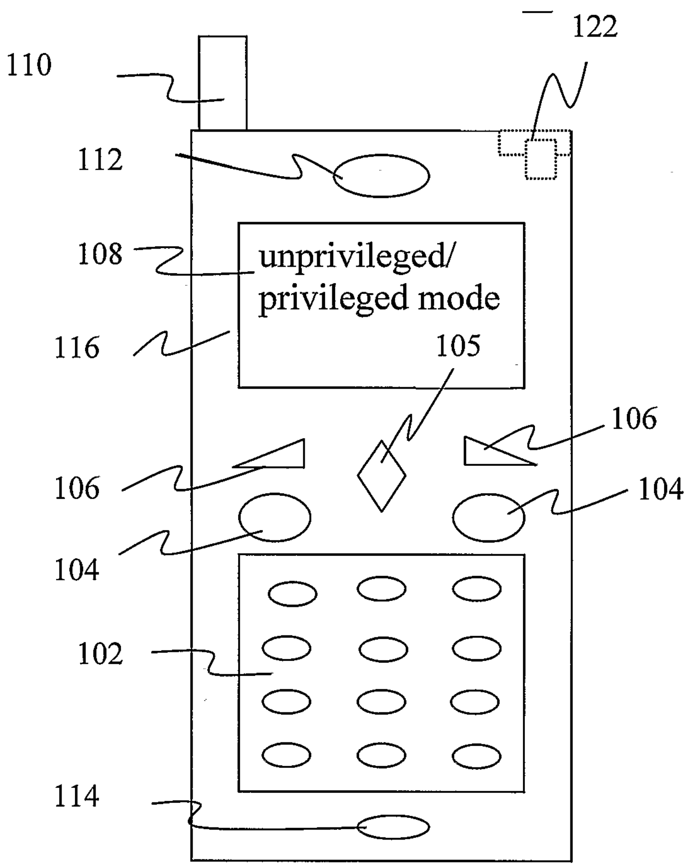

110
122
112
108
unprivileged/
privileged mode
116
105
106
106
104
104
102
114

Figure 1

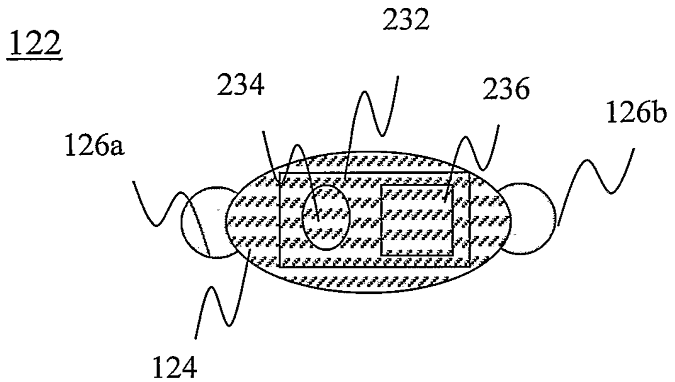


Figure 2a

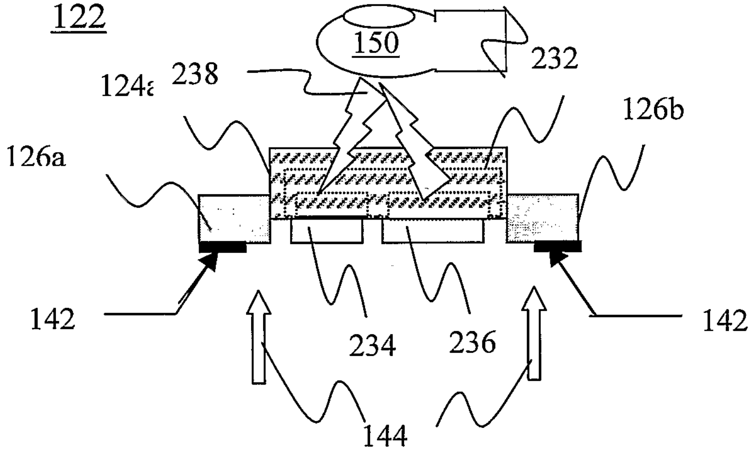


Figure 2b

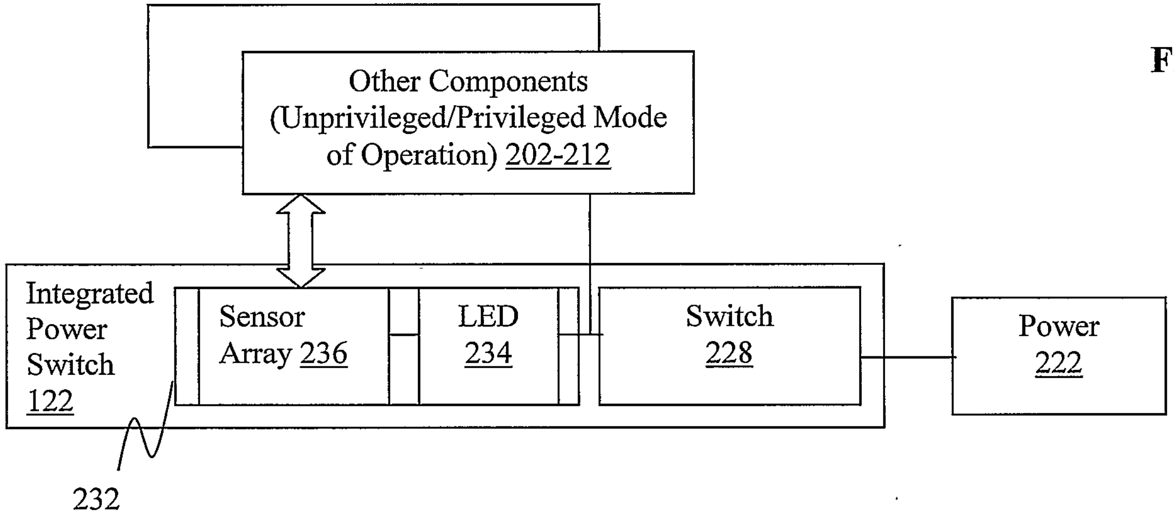


Figure 3a

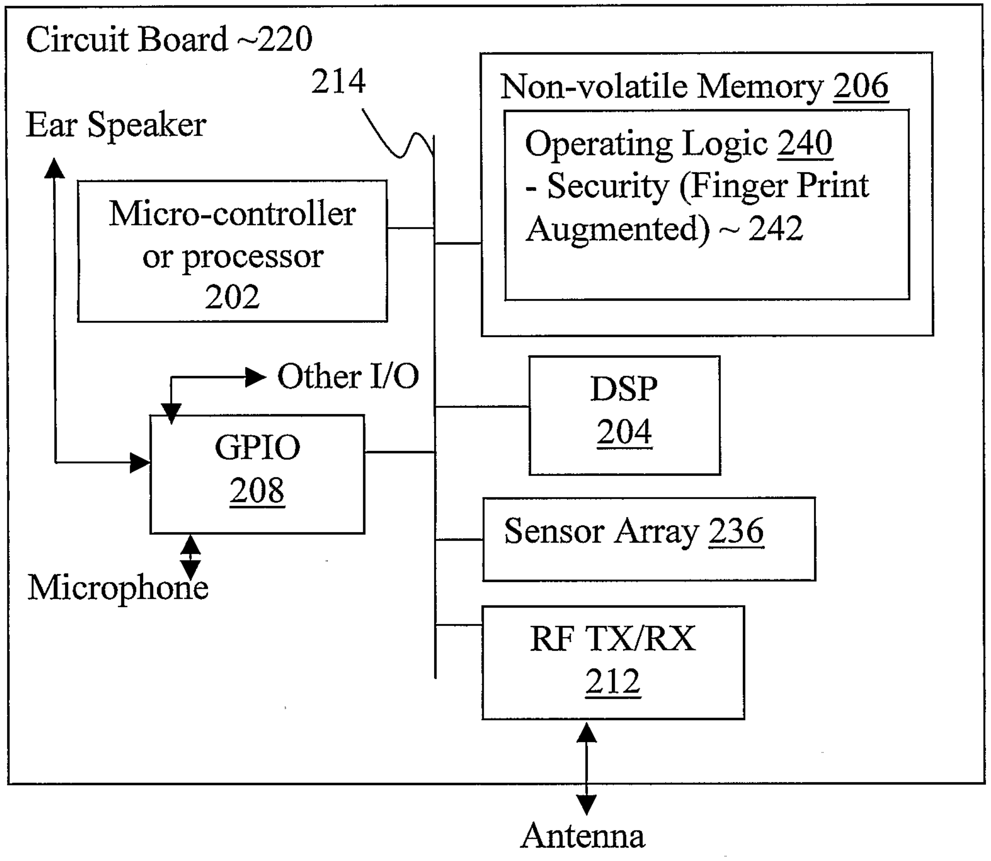

Circuit Board ~220
214
Ear Speaker
Micro-controller or processor 202
Other I/O
GPIO 208
Microphone
Non-volatile Memory 206
Operating Logic 240 - Security (Finger Print Augmented) ~ 242
DSP 204
Sensor Array 236
RF TX/RX 212
Antenna

Figure 3b

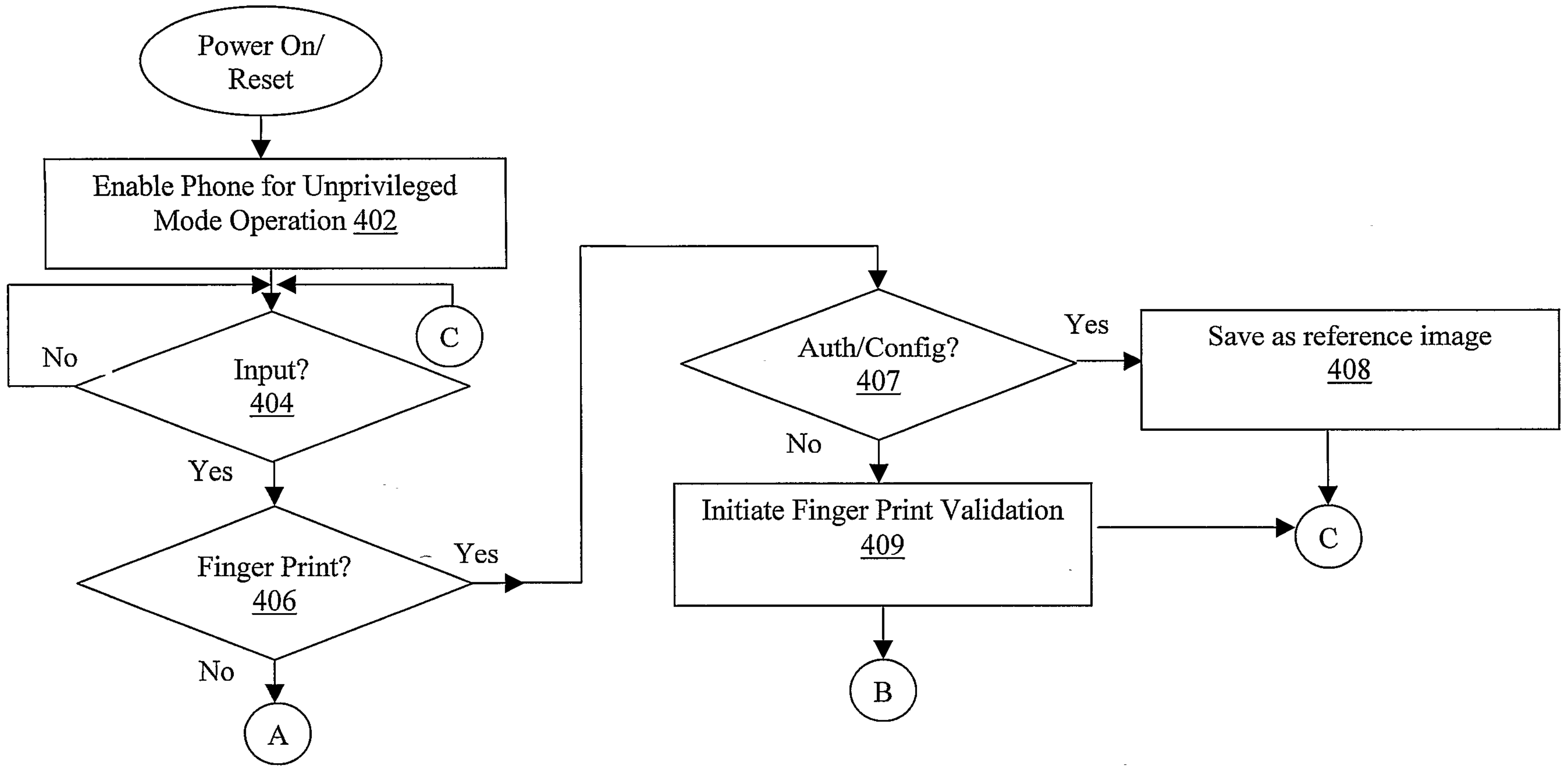

Power On/ Reset
Enable Phone for Unprivileged Mode Operation 402
No
Input? 404
C
Yes
Finger Print? 406
Yes
No
A
Auth/Config? 407
Yes
Save as reference image 408
No
Initiate Finger Print Validation 409
C
B

Figure 4a

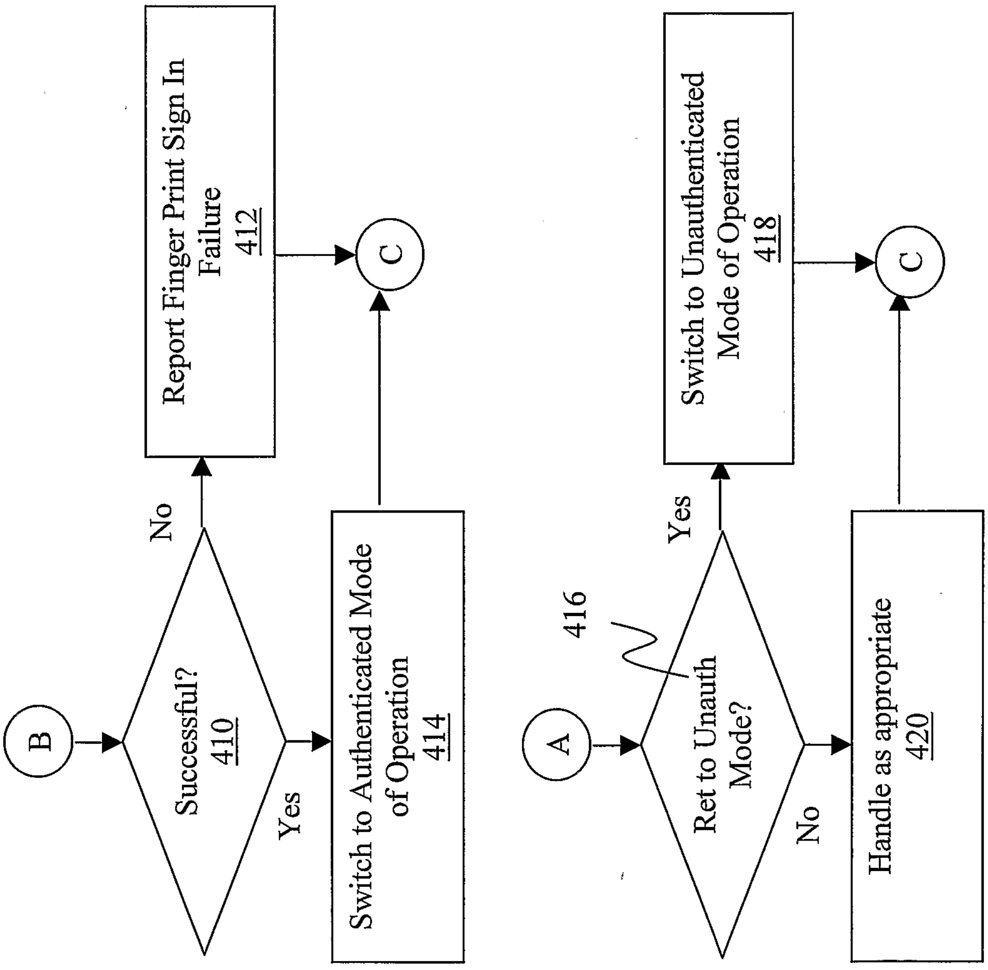

B
Successful?
410
No
Yes
Report Finger Print Sign In Failure
412
C
Switch to Authenticated Mode of Operation
414
A
416
Ret to Unauth Mode?
Yes
No
Switch to Unauthenticated Mode of Operation
418
C
Handle as appropriate
420

Figure 4b

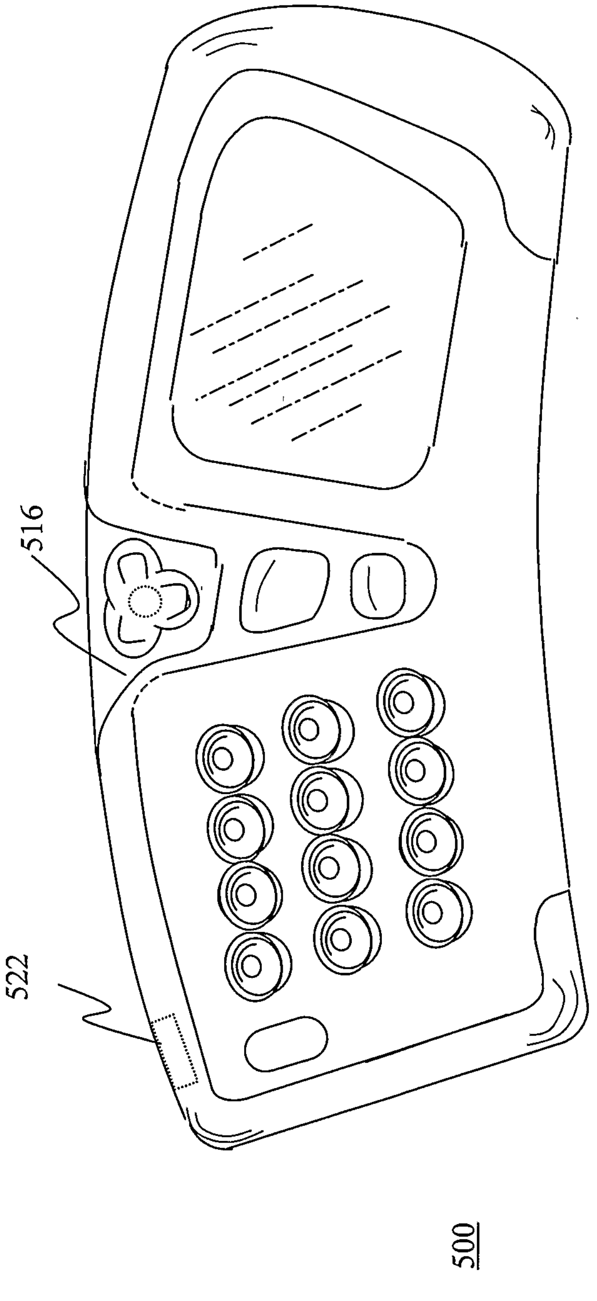


Figure 5

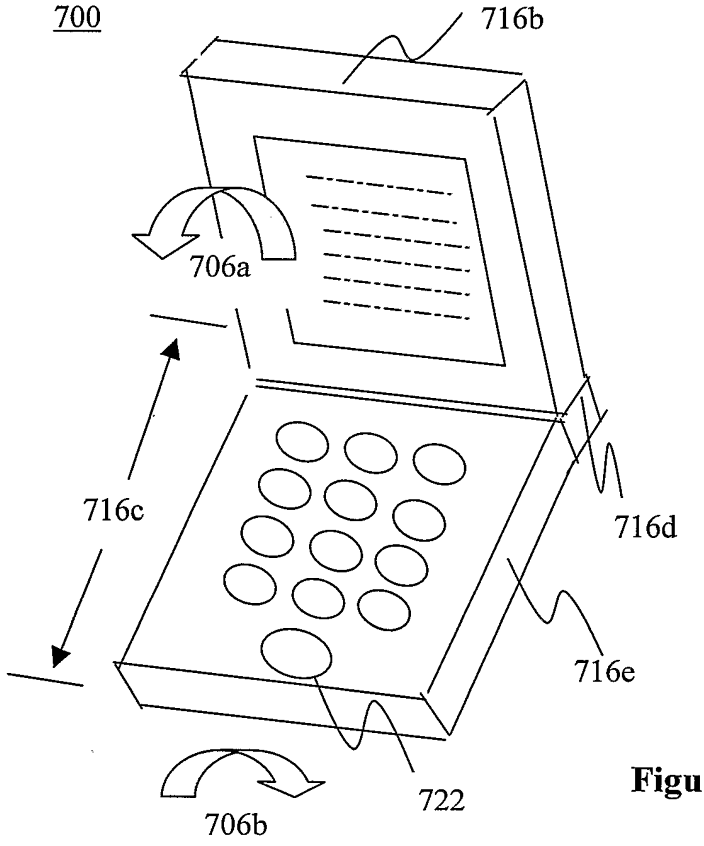


Figure 6a

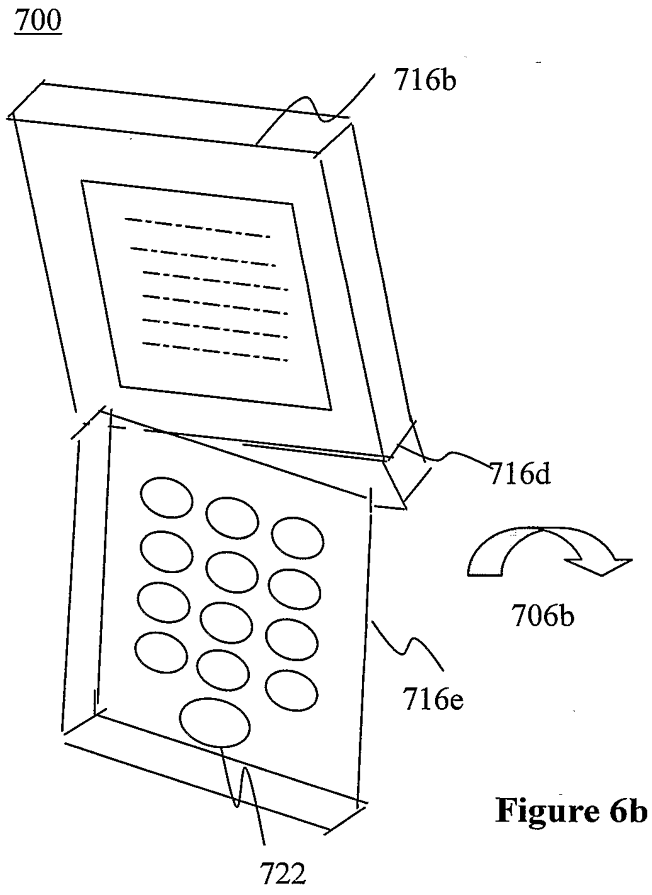


Figure 6b

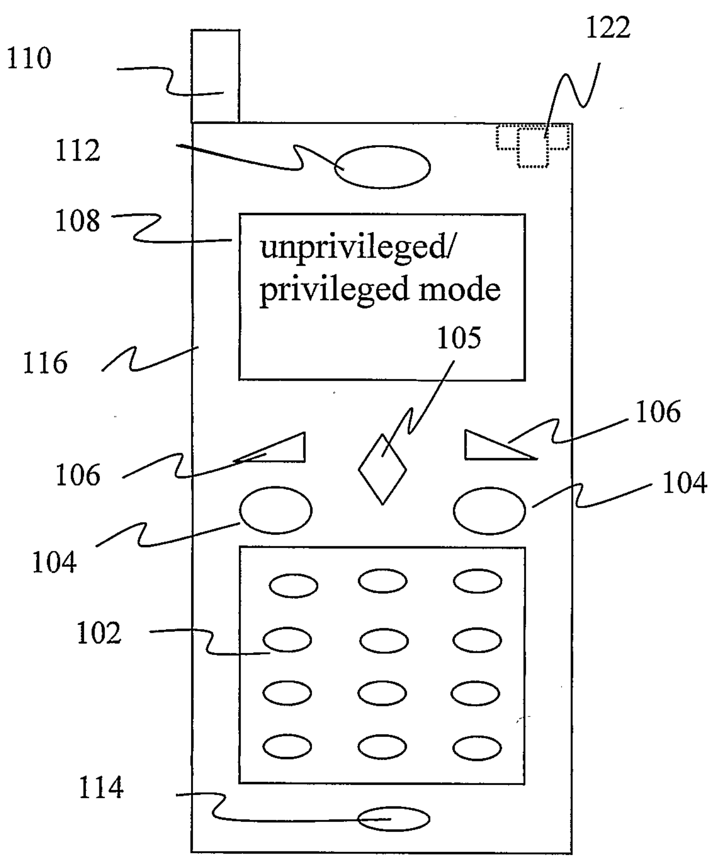


Figure 7a

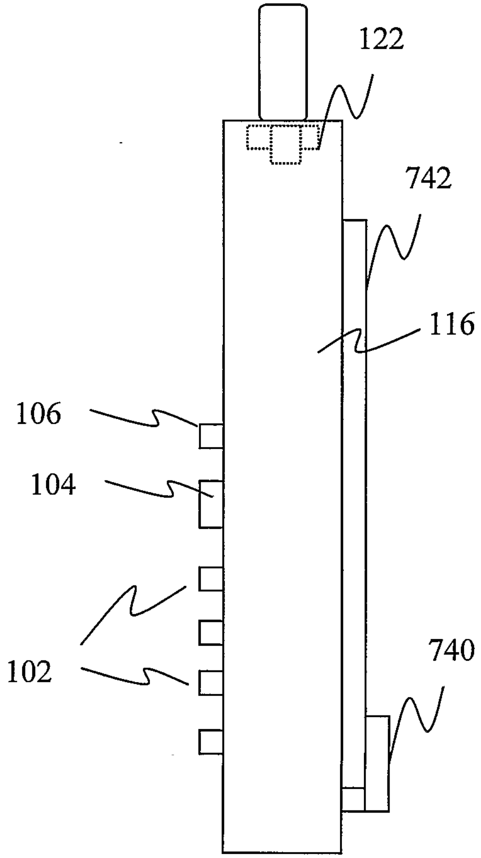


Figure 7b

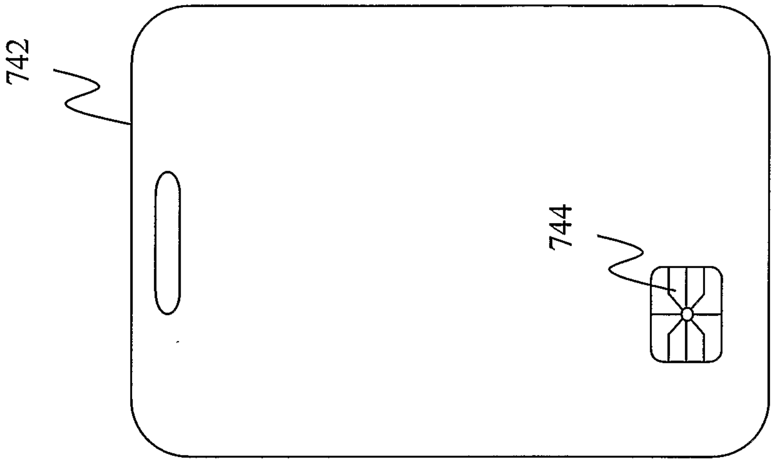


Figure 8b

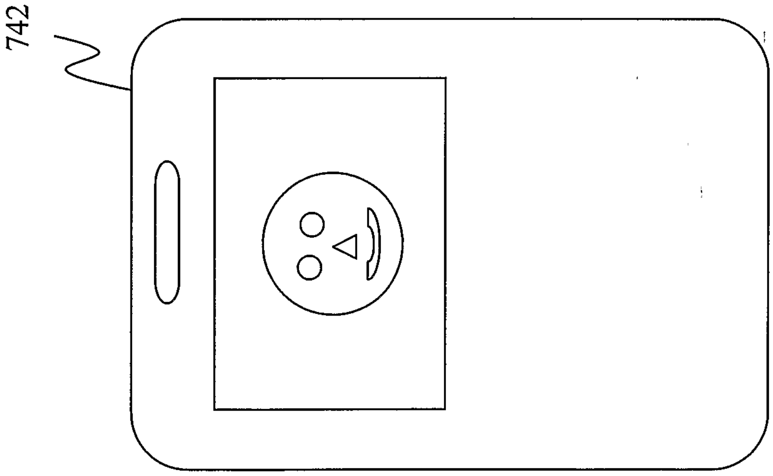


Figure 8a

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/09781

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20
US CL : 455/411

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/411, 410, 558, 556.1; 380/247, 249, 250

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0052192 A1 (YAMAZAKI et al.) 02 May 2002 (02.05.2002); paragraphs 0011, 0015, 0019, 0048, 0051, 0059	1-4, 9-11
X	US 2002/0083329 A1 (KIYOMOTO) 27 June 2002 (27.06.2002); paragraphs 0001, 0008, 0032, 0035, 0038	1-4, 9-11
X	US 5,913,175 (PINAULT) 15 June 1999 (15.06.1999); abstract; col. 3: line 49 - col. 4: line 5; col. 7: lines 39-50	14-17

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
13 July 2004 (13.07.2004)

Date of mailing of the international search report
03 AUG 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Erika A. Gary
Eugenia Logan
Telephone No. 703-305-4750