



US 2010093395A1

(19) **United States**(12) **Patent Application Publication**
Cocita(10) **Pub. No.: US 2010/0093395 A1**(43) **Pub. Date: Apr. 15, 2010**(54) **SAFEGUARDING USER DATA STORED IN
MOBILE COMMUNICATIONS DEVICES****Publication Classification**(76) Inventor: **Keith Cocita**, Santa Cruz, CA (US)(51) **Int. Cl.****H04M 1/00**

(2006.01)

G06F 12/16

(2006.01)

Correspondence Address:

PATENT LAW PROFESSIONALS**P.O. BOX 612407****SAN JOSE, CA 95161 (US)**(52) **U.S. Cl. 455/557; 710/304; 707/610; 711/162**(21) Appl. No.: **12/637,560**(22) Filed: **Dec. 14, 2009****Related U.S. Application Data**

(60) Continuation of application No. 11/112,020, filed on Apr. 21, 2005, which is a division of application No. 10/405,348, filed on Apr. 1, 2003, now Pat. No. 7,054,624.

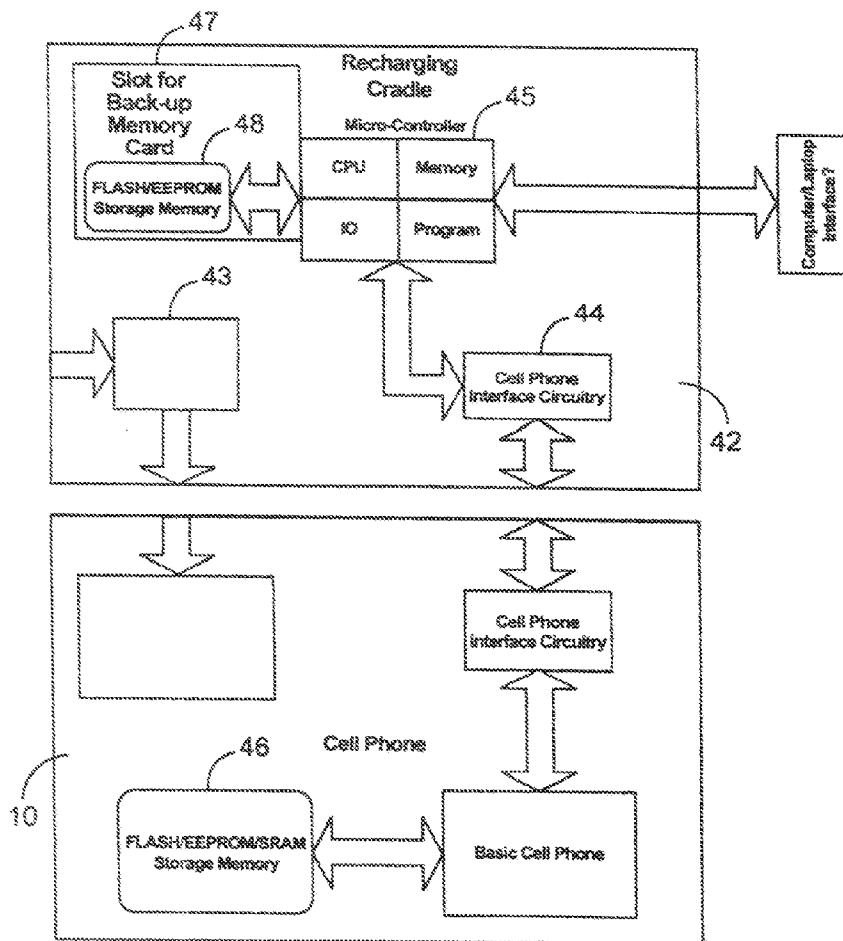
(60) Provisional application No. 60/369,431, filed on Apr. 2, 2002.

(57)

ABSTRACT

A docking apparatus for a portable communications device includes a cradle adapted to receive and hold a portable communications device, a memory card slot adapted to receive an erasable nonvolatile memory card, and circuitry configured to synchronize private user data stored in a memory of the portable communications device with private user data stored in the erasable nonvolatile memory card. The private user data is being held in the cradle of the portable communications device and after the erasable nonvolatile memory card is inserted in the memory card slot of the docking apparatus.

**Cell Phone Recharging Cradle
Block Diagram**



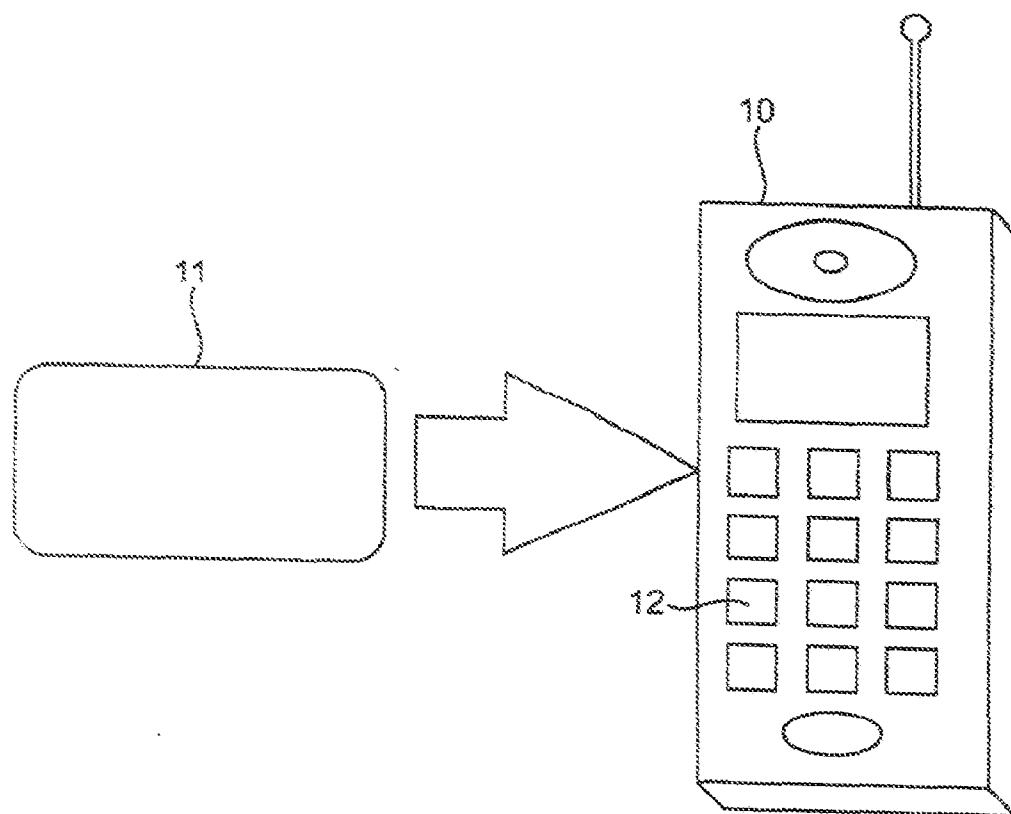


FIG. 1

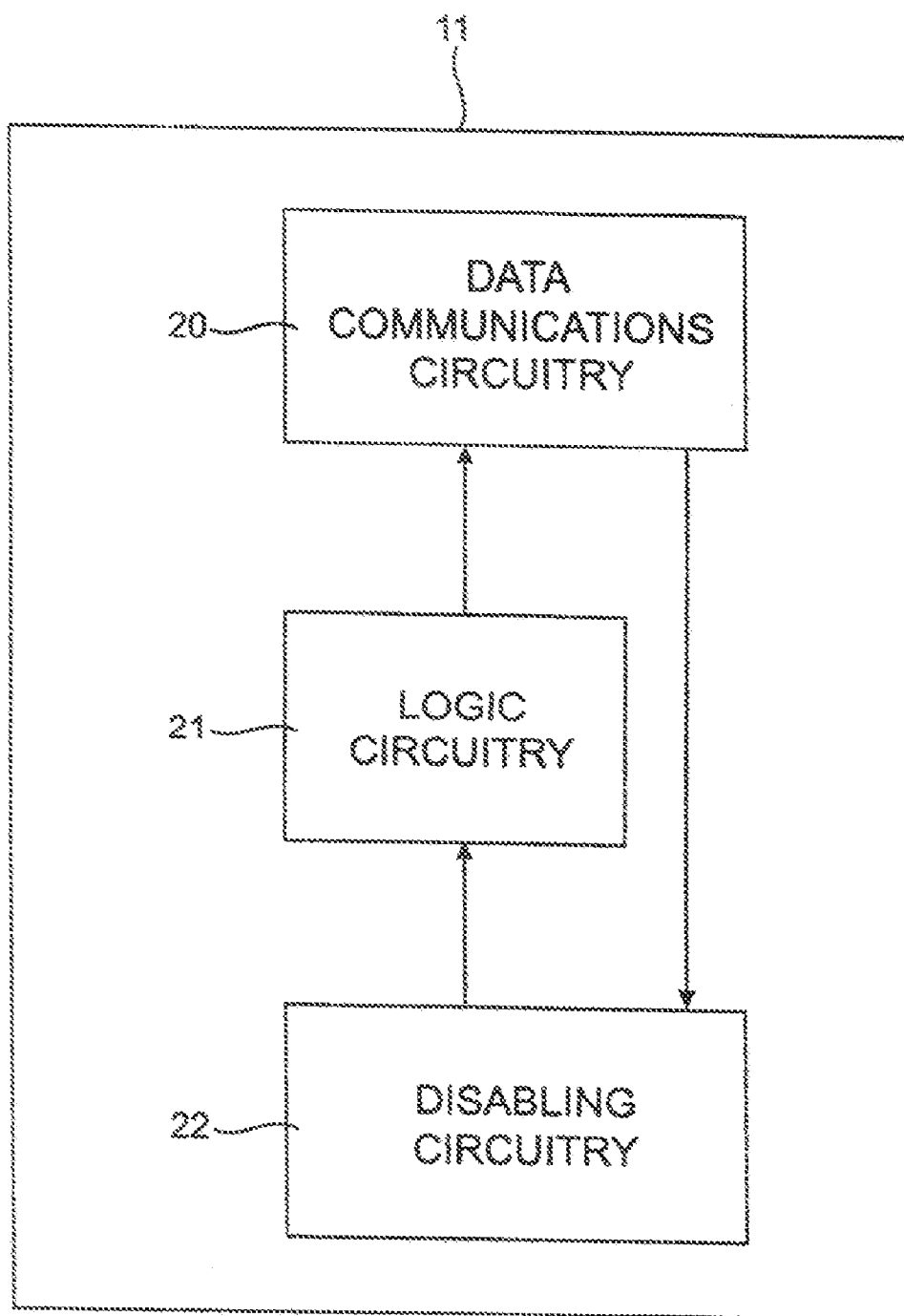
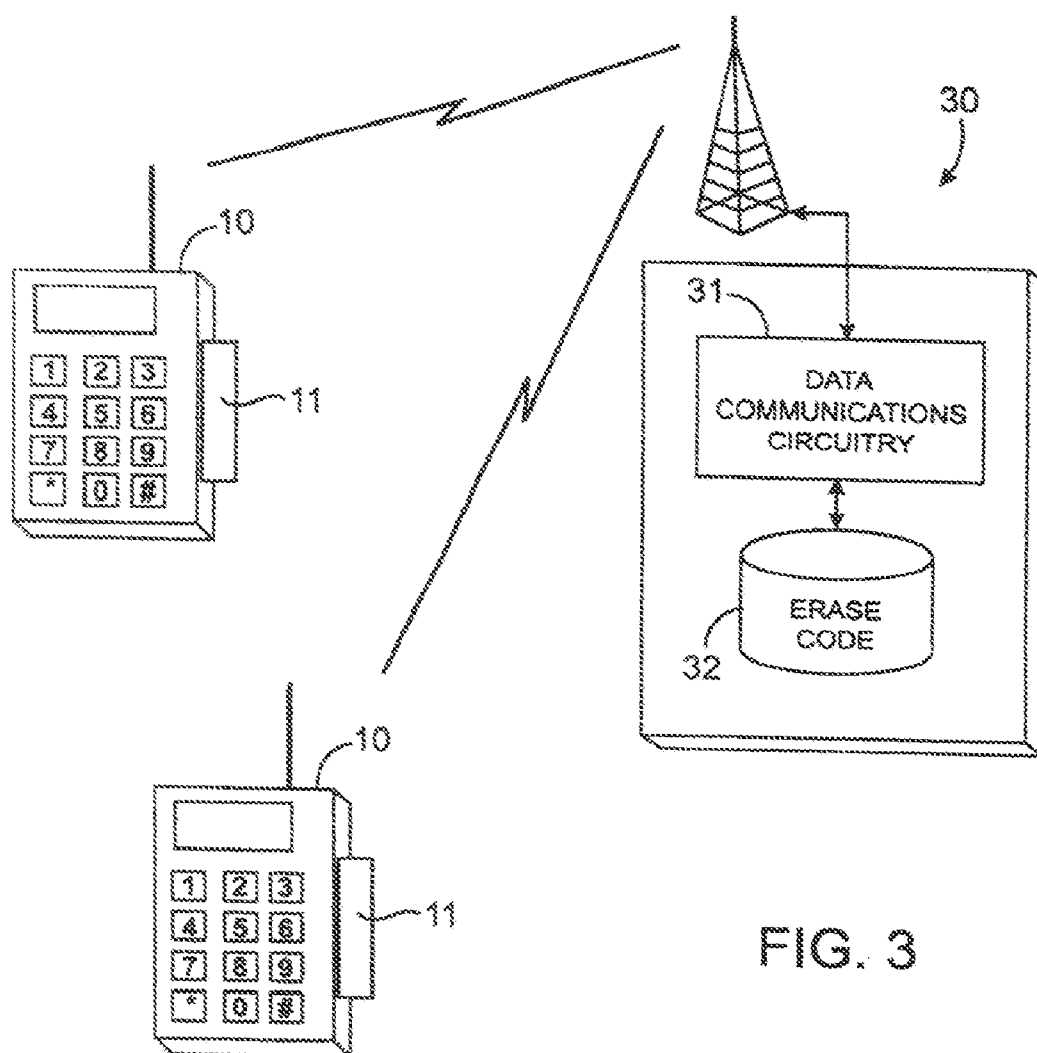


FIG. 2



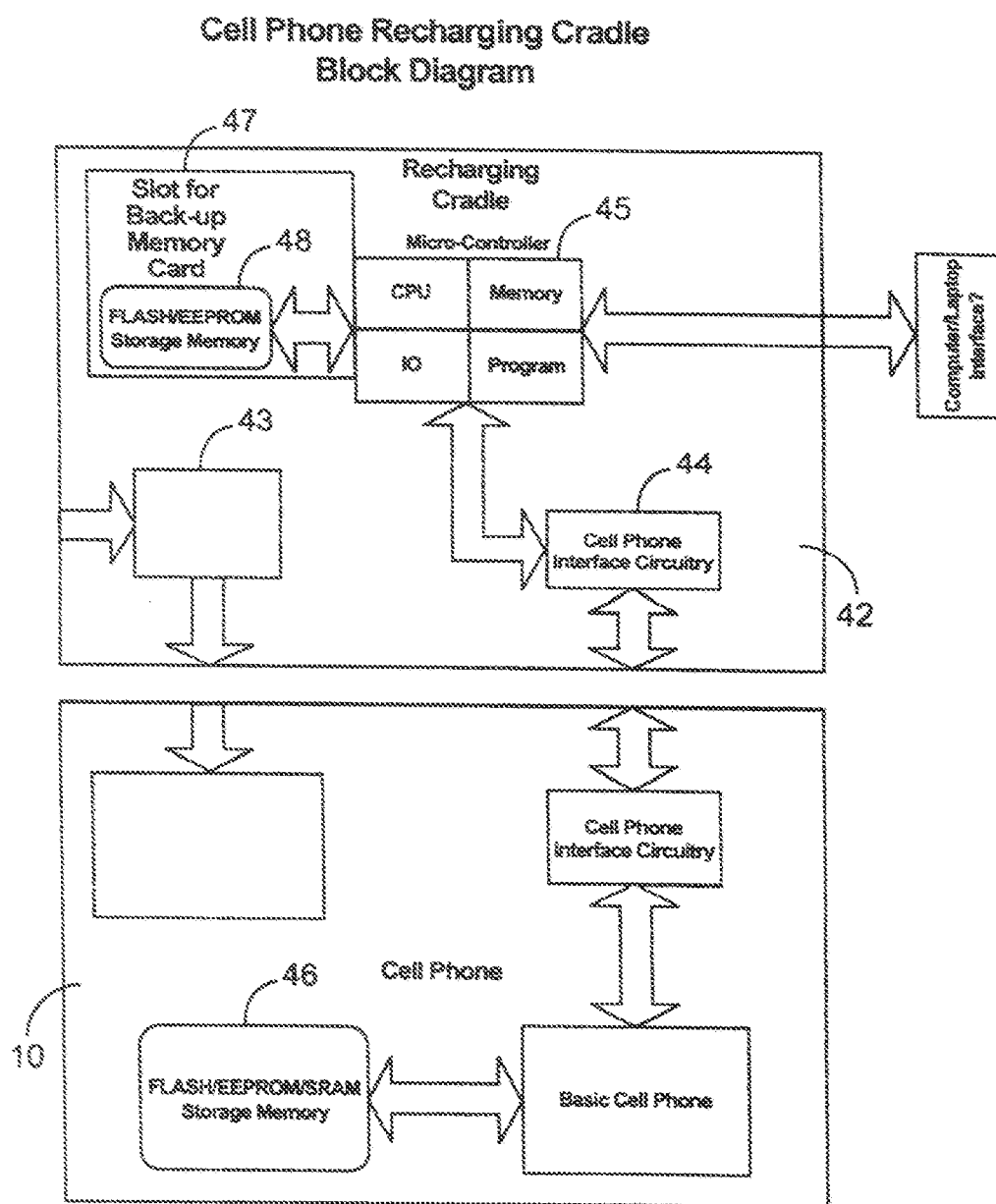


FIG. 4

SAFEGUARDING USER DATA STORED IN MOBILE COMMUNICATIONS DEVICES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation of U.S. patent application Ser. No. 11/112,020, filed on Apr. 21, 2005, which is a division of U.S. patent application Ser. No. 10/405,348, filed on Apr. 1, 2003, which claims the benefit of U.S. Provisional Patent Application No. 60/369,431, filed on Apr. 2, 2002, the disclosures of which are hereby incorporated by reference in their entireties for all purposes.

FIELD OF THE INVENTION

[0002] The present invention is directed to cell phones with memory, and to a method and apparatus for safeguarding the private, owner information entered into the cell phone memory, and to the use of a telecommunications network to remotely erase cell phone memory.

BACKGROUND OF THE INVENTION

[0003] Modern telecommunications networks include mobile stations, such as cell phones, which utilize a SMARTCARD which includes a SIM (subscriber identity module). The SIM's have a memory chip that contains data such as the identity of the card holder (i.e., the service subscriber), billing information, and home location. When a cell phone user places a call, the SIM communicates the unique SIM code to the network. The network checks to see if the SIM code owner is a current subscriber to the network service, often by matching the SIM code with a list of authorized SIM codes. This authentication, or matching of SIM codes generally precedes all other network communication with the cell phone.

[0004] SMARTCARDS were developed to allow cell phone activities other than simple telephone calls. The SMARTCARD can contain microprocessors for, e.g., transaction management, data encryption and user authentication. The SMARTCARD or the SIM may include subscriber entered telephone numbers and other valuable information. Theft of the phone places this valuable information in the hands of others. In fact, the loss of the phone is probably less important than the loss of the valuable information contained therein. This is especially true for the new cell phones which now access the Internet, and for cell phones coupled with handheld computing devices, which browse the Internet, store Power Point presentations, and do rudimentary word processing, as well as scheduling appointments and maintaining expense accounts.

[0005] Many security features have been developed for cell phones. Most of these are related to prevention of theft of communication services by permanently disabling a stolen phone, temporarily disabling a phone for which the subscriber is in arrears, or blocking calls to geographical regions which are not part of the subscriber's contract.

[0006] U.S. Pat. No. 5,898,783 discloses a telecommunications network with disabling circuitry which can disable the SMARTCARD of the cell phone of a particular subscriber. The disable command can permanently incapacitate the SMARTCARD by destroying the power connection for the logic circuitry, or temporarily incapacitate the logic circuitry by erasing the memory within the card. According to this patent, the numbers of stolen phones can be reported to the network and entered into a database which is searched when any cell

phone requests service, and a disable command or signal returned to the cell phone if its number is in the disable database. In the present invention, the subscriber erases the memory containing the private information without the additional steps and involvement of the network, giving the subscriber greater freedom and opportunity to safeguard their private information.

[0007] U.S. Pat. No. 5,734,978 describes a telecommunications system having a manufacturer preset destruct code stored in each cell phone. When a subscriber reports a phone stolen, the network's base station controller initiates a destruct program, using the destruct code. The destruct code destroys the data necessary for performing the telephone functions, but not the private data.

[0008] U.S. Pat. No. 6,259,908 describes a cellular phone system in which a locking code on a particular cell phone may be erased by means of a message transmitted through the cell phone system, but may not be erased or changed using the keyboard features of that phone. This arrangement has particular usefulness in a designated cellular system with many units, such as a communications network for the fire department of a large city. To set up or reconfigure the network, the entire network must be activated and the individual units (cell phones) assigned a particular number. According to the patent, all phones on the system have a locking code to prevent theft communications on the network until all units are assigned. This is a subscriber system approach to preventing theft of service of the communications system, and does not relate to the privacy of data of individual subscribers.

SUMMARY OF THE INVENTION

[0009] It is an object of the present invention to safeguard the private data entered into a cell phone by its owner, by permitting the owner to erase or destroy that data using an on-air signal. According to the present invention, the memory chip of a cellular phone on which private data is recorded may be provided with an erase means. This erase means could comprise a fuse, switch, or similar device in a disable, or erase, circuit. The erase means executes an erase command on receiving an on-air erase code which matches the erase code preset by the owner. If the mobile phone is lost or stolen, the owner need only call the telephone number of the lost or stolen phone and enter the erase code. The private data will be erased. Thus, the owner can protect the phone numbers and the addresses of family, friends and associates. If the owner believes the phone has been misplaced, he can destroy the private information without disabling the telephone features, should the missing phone be found.

[0010] It is also an object of the present invention to maintain the privacy and integrity of the cell phone owner's data, as well as to facilitate its transfer to a new cell phone. The integrity of the private data can be maintained with a novel recharging cradle or station. According to the present invention, the cell phone recharging cradle or station may incorporate a slot for a memory device, such as a PCMCIA card, which communicates with a phone docked in the cradle. Every time the phone is placed in the cradle for recharging the PCMCIA card does a check sum of the phone's memory. If numbers or other data have been entered into the phone, the card downloads that information so that the card is always updated. When a new phone is charged in the base station, the check sum is started, and all private data entered into the previous phone is automatically uploaded into your new phone. Using this system, if the user does not want anyone

else to have access to their numbers they may simply remove the PCMCIA card from the phone. Also, a backup card can be easily carried in a wallet, when traveling.

[0011] These objects, as well as other objects which will become apparent from the discussion that follows, are achieved, in accordance with the present invention, which comprises a cell phone programmable memory chip with erase means; a recharging cradle with slot for, e.g., a PCMCIA card, which can upload data from, or download data into, a cell phone docked therein; and a cell phone apparatus with a) first memory for storing the unique identification numbers of the apparatus, b) transmitting/reception means for transmitting and receiving a call in accordance with said identification numbers, c) an EEPROM with a programmable data base for data, and a predetermined address (or memory location) for an erase code, d) means for entering erase code at the predetermined location, and e) erasing means for erasing said database on receipt of the erase code.

[0012] These objects are also achieved by the method of the present invention, for safeguarding private data stored in a selected cell phone on a mobile telecommunications system which comprises a plurality of individual mobile cell phone apparatus and a mobile telephone switching office, said at least one selected apparatus having a PROM for storing private data including an erase code, and a unique telephone number, said method comprising receiving at the selected mobile phone apparatus, from the switching network, a message containing the erase code from the switching network, and erasing the private data.

[0013] For a full understanding of the present invention, reference should now be made to the following detailed description of the preferred embodiments of the invention as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 illustrates a cell phone, or mobile telecommunications apparatus, and the SMARTCARD that is received therein, which cooperates with the cell phone to effect communication with a telecommunications network.

[0015] FIG. 2 illustrates a block diagram of a SMARTCARD according to the principles of the present invention.

[0016] FIG. 3 illustrates a block diagram of a telecommunications network capable of communicating with a plurality of cell phones that cooperate with a SMARTCARD to effect communication with the telecommunications network.

[0017] FIG. 4 illustrates a block diagram of a cell phone re-charging cradle according to one embodiment of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] The preferred embodiments of the present invention will now be described with reference to FIGS. 1-4 of the drawings. Identical elements in the various figures are designated with the same reference numerals.

[0019] As shown in FIG. 1, the cell phone 10 receives the SMARTCARD 11 which cooperates with the cell phone to effect communication with a telecommunications network, such as that illustrated in FIG. 3. The SMARTCARD, includes a SIM (subscriber identity module). The SMARTCARD identifies the user of the telecommunications system, and serves to authenticate the user as one permitted on the network. The SMARTCARD may also encrypt communica-

tions between the cell phone 10 and the telecommunications network. The alphanumeric keys, 12 of the cell phone may be used to enter information into the cell phone memory, and are the preferred means for entering the erase code.

[0020] The elements of the SMARTCARD, illustrated in FIG. 2, include a data communications circuitry, a logic circuitry and a disabling, or erasing, circuitry. The data communications circuitry, 20, transmits a code uniquely identifying the SMARTCARD. The logic circuitry, 21, in the present embodiment includes data processing and storage circuitry and interconnecting circuitry, including, without limitation, a processor, memory, support circuitry, and any address, data and control buses (not shown). In one embodiment of the present invention the logic circuitry encrypts communication between the cell phone and the telecommunications network. As cell phones develop, the logic circuitry may be used to perform more and more functions, without affecting the features of the logic circuitry essential to the present invention.

[0021] The card is provided with disabling circuitry, 22, which can e.g., permanently erase the memory of the card. The disabling circuitry may comprise either a fuse or a switch, which operates to e.g. decouple the electrical power from the memory in card. Other means of effectively erasing the memory are known to those in the art, as by providing an excessive voltage that causes the memory to malfunction, even if it is still receiving power, or permanently incapacitating the logic circuitry by cutting it off from its source of power.

[0022] A block diagram of the telecommunications network is illustrated in FIG. 3. The telecommunications network, 30 is capable of communication with a plurality of cell phones 10 with cards, 11, having a subscriber identity module. Each card has a unique SIM code. Upon initiation of access to the network, the SIM code is transmitted to the network. The network, 30 has data communications circuitry, 31, to receive the SIM code. In one embodiment of the invention, the network may also include a PROM or an EEPROM for receiving and storing an erase code associated with a unique SIM code. In another embodiment of the invention, the data communications circuitry, 31, may also include an erase command.

[0023] The operation of the method and apparatus of the present invention will now be described. The user of SMARTCARD may use the alphanumeric keys, 12 to enter into, and store in the memory, an erase code to permit erasure of private data in the phone. According to a preferred embodiment of the present invention, the erase code for any selected cell phone may only be directly entered into the phone, using the keypad for that phone. The erase code may be stored in memory on the SMARTCARD, or may be transferred to, and stored on, the network. The erase code for a particular SMARTCARD or SIM may not be preset or changed by an on-air signal from a cell phone with a different SIM. The erase command maybe included in the data communications circuitry of the card or on the network.

[0024] If the cell phone is stolen or lost, the user may, using another cell phone or a land line, call the telephone number of the stolen or lost cell phone, and enter the erase code. The data communications circuitry of the network and the lost phone "matches" the erase code of the on-air communication with the preset stored erase code. The "matching" may involve an exact matching of characters, or an exact mapping, requiring a specific relationship, between the preset erase code and the received erase code. If there is a match, an erase command is

issued, and the private data in the stolen or lost cell phone is erased. The circuitry for executing the erase command is in the cell phone.

[0025] The present invention does not require a network database of erase codes, permitting great individual privacy. In addition, the user does not need to access disable commands on the network. No database of disabled numbers needs to be assembled and maintained by and at the network in order for the user to disable the memory for his private data. When the erase code is stored in the cell phone, it is instantly operable. In addition it may be instantly changed. The privacy of data entered into cell phones is of increasing importance. New phones incorporate Internet text messaging, e-mail, and web surfing and downloading. Elaborate negotiations may now be conducted via a cell phone. In addition, cell phones are being combined with handheld computers and organizers, which contain word processing. Entire contracts may be recorded, transmitted, or received on a handheld apparatus including a cell phone on a telecommunications network.

[0026] FIG. 4 illustrates a preferred embodiment of a recharging cradle, 42, according to the present invention. The cradle includes recharging circuitry, 43, which connects to the phone, 10, when the phone is in the dock, as shown in FIG. 4. Also included in the cradle is cell phone interface circuitry, 44, which comprises an upload/download cell phone memory device, comprising a micro-controller, 45, which comprises a CPU, a memory, IO (input output) and the program or application. The program compares the memory in the phone memory, as shown here as the erasable FLASH/EEPROM/ SRAM storage memory, 46, which is part of the present invention, with the memory in the cradle, as with a check sum operation; and downloading to the cradle memory any numbers which have been added to the phone, and uploading to the phone any numbers in the cradle memory which are not in the phone.

[0027] As shown in FIG. 4, the recharging cradle may further comprise an upload/download slot, 47, for a back-up cell phone memory device, 48. The slot comprises a micro-controller, and interface circuitry in communication with either the memory in a docked cell phone, or, as shown, with the memory in the cradle. The back-up memory device may be any device suitable for insertion into a new phone, such as a PCMCIA card. As shown in FIG. 4, this PCMCIA card is provided with an erasable memory.

[0028] These back-up devices provide a very convenient means for maintaining the integrity of private data for the cell phone. If the cell phone is stolen or lost, no time need be taken in an attempt to recover the stored private data, but the private data immediately erased, as a duplicate copy exists in the cradle, and optionally on the back-up PCMCIA. The back-up PCMCIA is easily stored in a wallet, while traveling, and may be placed into a new cell phone, or the PCMCIA card kept in the cradle, and data therein transferred to a new cell phone docked in the cradle. If the new cell phone has to be initially charged, charging in the cradle with PCMCIA card slot will enter all the private data into the new cell phone.

[0029] In another aspect of the present invention, a novel recharging cradle for the cell phone may be provided with an upload/download slot for receiving an additional memory device or card, such as a PCMCIA card, for maintaining the integrity of private data for the cell phone. The slot comprises a micro-controller, crystal and interface circuitry, connecting the memory device in the slot and the memory device in the phone. Once placed in the slot, the e.g. PCMCIA card is in

communication with any cell phone docked in the cradle. On docking the cell phone in the cradle a check sum may be initiated, and any new data from the cell phone added to the PCMCIA card. Then, should the cell phone be stolen or lost, no time for recovery of the stored private data need be allotted, but the private data immediately erased, as a duplicate copy exists on the spare PCMCIA. The spare PCMCIA is easily stored in a wallet, while traveling, and may be placed into a new cell phone, or the PCMCIA card kept in the cradle, and data therein transferred to a new cell phone docked in the cradle. If the new cell phone has to be initially charged, charging in the cradle with PCMCIA card slot will enter all the private data into the new cell phone.

[0030] Those skilled in the art should understand that while the present invention may be embodied in hardware that alternative embodiments may include software or firmware, or combinations thereof. Such embodiments may include implementations using conventional processing circuitry such as, without limitation, programmable array logic ("PAL"), digital signal processors ("DSPs"), field programmable gate array ("FPGA"), application specific integrated circuits ("ASICs"), large scale integrated circuits ("LSIs"). Moreover, the present embodiment is introduced for illustrative purposes only and other embodiments that provide a system for and method of disabling a SIM card are well within the broad scope of the present invention. Conventional computer, and processing, system architecture is more fully discussed in Computer Organization and Architecture, by William Stallings, MacMillan Publishing Co. (3rd ed. 1993). Conventional processing system network design is more fully discussed in Data Network Design, by Darren L. Spohn, McGraw-Hill, Inc. (1993). Conventional voice and data communications are more fully discussed in Data Communications Principles, by R. D. Gitlin, J. F. Hayes and S. B. Weinstein, Plenum Press (1992), The Irwin Handbook of Telecommunications, by James Harry Green, Irwin Professional Publishing (2nd ed. 1992) and Voice & Data Communications Handbook, by Regis J. Bates, Jr. and Donald Gregory, McGraw-Hill (1996). Conventional electronic circuit design is more fully discussed in The Art of Electronics, by Paul Horowitz and Winfield Hill, Cambridge University Press, (2nd ed. 1989). Conventional control systems and architectures are discussed in Modern Control Engineering by Katsuhiko Ogata, Prentice Hall 1990. Each of the foregoing publications is incorporated herein by reference.

[0031] There has thus been shown and described a novel method and apparatus for both safeguarding and maintaining the integrity of the private data in a cell phone memory, which fulfills all the objects and advantages sought therefor. Many changes, modifications, variations and other uses and applications of the subject invention will, however, become apparent to those skilled in the art after considering this specification and the accompanying drawings which disclose the preferred embodiments thereof. All such changes, modifications, variations and other uses and applications which do not depart from the spirit and scope of the invention are deemed to be covered by the invention, which is to be limited only by the claims which follow.

What is claimed is:

1. A method of creating a backup of user data stored in a memory of a mobile communications device, comprising:
when said mobile communications device is coupled to a recharging cradle, downloading to a cradle memory integrated in said recharging cradle user data stored in a

memory of said mobile communications device that is not stored in the cradle memory; and
 uploading a complete backup of user data stored in the cradle memory to a backup memory card plugged into a memory card slot of the recharging cradle.

2. The method of claim 1, further comprising:
 if said mobile communications device is lost or stolen,
 downloading to the cradle memory user data stored in the backup memory card; and
 uploading to a memory of a second mobile communications device the user data in the backup memory card that has been downloaded to the cradle memory.

3. The method of claim 1 wherein the backup memory card comprises a memory card adapted to be inserted into a memory slot of a second mobile communications device, in the event the first mobile communications device is lost or stolen.

4. The method of claim 1 wherein user data stored in the memory of said mobile communications device, cradle memory and backup memory card comprises private user data.

5. The method of claim 4 wherein said private user data comprises one or more telephone numbers.

6. A docking apparatus for a communications device, comprising:
 a cradle having an electrical interface adapted to couple to an electrical connection of a communications device and a memory card slot adapted to receive a backup memory card;
 a cradle memory configured within said cradle operable to store private user data;
 means for downloading private user data stored in a memory device of the communications device but not in the cradle memory from the memory device of the communications device to the cradle memory when the electrical connection of the communications device is coupled to the electrical interface of the cradle; and
 means for uploading a complete backup copy of the private user data stored in the cradle memory in a backup memory card plugged into the memory card slot of the cradle.

7. The docking apparatus of claim 6, further comprising means for uploading private user data stored in the cradle

memory but not in the memory device of the communications device from the cradle memory to the memory device of the communications device when the electrical connection of the communications device is coupled to the electrical interface of the cradle.

8. The docking apparatus of claim 6 wherein the communications device comprises a mobile communications device.

9. The docking apparatus of claim 6 wherein said private user data comprises one or more telephone numbers.

10. A docking apparatus for a portable communications device, comprising:

a cradle adapted to receive and hold a portable communications device;

a memory card slot adapted to receive an erasable nonvolatile memory card; and

circuitry operable to synchronize private user data stored in a memory of said portable communications device with private user data stored in the erasable nonvolatile memory card when the erasable nonvolatile memory card is inserted in said memory card slot and the portable communications device is being held in said cradle.

11. A method of recovering private user data stored in a communications device, in the event that the communications device is lost or stolen, said method comprising:

docking a first communications device in a cradle, said cradle having a cradle memory and circuitry for synchronizing private user data stored in a memory of a first communications device with private user data stored in the cradle memory;

synchronizing the private user data stored in said first communications device with the private user data stored in the cradle memory;

creating a duplicate of the synchronized private user data in a memory card;

storing the memory card in a location separate from the first communications device; and

in the event that the first communications device is lost or stolen, inserting the memory card in a second communications device to recover the synchronized private user data.

* * * * *