**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 | A1

(11) International Publication Number: **WO 97/18653**

(43) International Publication Date: 22 May 1997 (22.05.97)

(21) International Application Number: PCT/US96/17902

(22) International Filing Date: 12 November 1996 (12.11.96)

(30) Priority Data:
08/558,091 13 November 1995 (13.11.95) US

(71) Applicant: TRANSACTION TECHNOLOGY, INC. [US/US]; 3100 Ocean Park Boulevard, Santa Monica, CA 90405 (US).

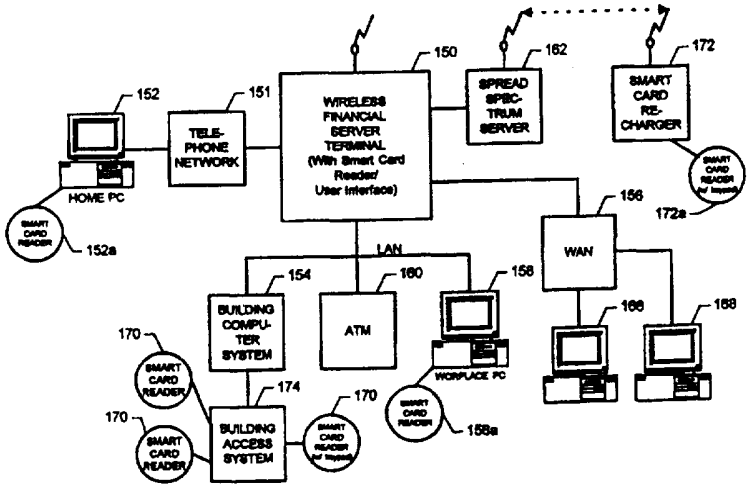
(72) Inventor: KAWAN, Joseph, C.; 2034 Paramount Drive, Hollywood, CA 90068 (US).

(74) Agent: HOGUE, Dale, Curtis, Sr.; Kilpatrick & Cody, L.L.P., Suite 800, 700 13th Street, N.W., Washington, DC 20005 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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 the receipt of amendments.*

(54) Title: WIRELESS TRANSACTION AND INFORMATION SYSTEM




(57) Abstract

A financial information and transaction system utilizes wireless communication (20) in connection with portable terminals. In this system, a terminal (150) is connected to the financial institution via a wireless (102) or cellular telephone hook-up. Smart cards are utilized to verify authorization for transactions, thereby minimizing potential security problems which could otherwise result from use of a mobile terminal (150). Alternatively, a smart card is advantageously utilized not only for authorization, but also to maintain a secure record of available funds. The system not only provides the functionality of an ATM network, but also provides non-financial services, thereby forming an integrated system.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|---|---|---|---|---|---|
| **AM** | Armenia | **GB** | United Kingdom | **MW** | Malawi |
| **AT** | Austria | **GE** | Georgia | **MX** | Mexico |
| **AU** | Australia | **GN** | Guinea | **NE** | Niger |
| **BB** | Barbados | **GR** | Greece | **NL** | Netherlands |
| **BE** | Belgium | **HU** | Hungary | **NO** | Norway |
| **BF** | Burkina Faso | **IE** | Ireland | **NZ** | New Zealand |
| **BG** | Bulgaria | **IT** | Italy | **PL** | Poland |
| **BJ** | Benin | **JP** | Japan | **PT** | Portugal |
| **BR** | Brazil | **KE** | Kenya | **RO** | Romania |
| **BY** | Belarus | **KG** | Kyrgystan | **RU** | Russian Federation |
| **CA** | Canada | **KP** | Democratic People's Republic of Korea | **SD** | Sudan |
| **CF** | Central African Republic | | | **SE** | Sweden |
| **CG** | Congo | **KR** | Republic of Korea | **SG** | Singapore |
| **CH** | Switzerland | **KZ** | Kazakhstan | **SI** | Slovenia |
| **CI** | Côte d'Ivoire | **LI** | Liechtenstein | **SK** | Slovakia |
| **CM** | Cameroon | **LK** | Sri Lanka | **SN** | Senegal |
| **CN** | China | **LR** | Liberia | **SZ** | Swaziland |
| **CS** | Czechoslovakia | **LT** | Lithuania | **TD** | Chad |
| **CZ** | Czech Republic | **LU** | Luxembourg | **TG** | Togo |
| **DE** | Germany | **LV** | Latvia | **TJ** | Tajikistan |
| **DK** | Denmark | **MC** | Monaco | **TT** | Trinidad and Tobago |
| **EE** | Estonia | **MD** | Republic of Moldova | **UA** | Ukraine |
| **ES** | Spain | **MG** | Madagascar | **UG** | Uganda |
| **FI** | Finland | **ML** | Mali | **US** | United States of America |
| **FR** | France | **MN** | Mongolia | **UZ** | Uzbekistan |
| **GA** | Gabon | **MR** | Mauritania | **VN** | Viet Nam |

# WIRELESS TRANSACTION AND INFORMATION SYSTEM

## FIELD OF THE INVENTION

This invention relates to a system for providing information and performing financial transactions. In particular, it relates to a financial system which utilizes wireless, portable terminals for providing financial information and performing financial transactions.

## CROSS-REFERENCE TO RELATED APPLICATION

Reference is made to commonly owned co-pending application Serial No. 08/177,548 entitled "WIRELESS SCREEN TELEPHONE," the disclosure of which is incorporated by reference herein.

## BACKGROUND OF THE INVENTION

The proliferation of automated teller machines (ATMs) has revolutionized the banking and financial services industry by increasing the ability to provide financial services to the consumer. For example, in the past virtually all consumer transactions were conducted in person. Thus, consumer access was generally limited to the business hours of branch locations. With the advent of ATM and other financial networks, consumers may now access financial services virtually twenty-four hours a day, seven days a week. This results in increased

convenience and efficiency both for the service provider and the consumer.

Despite these successes, ATM and other financial networks in use today are characterized by certain shortcomings which limit consumer access and provide a barrier to more widespread accessibility and use. For example, the ATMs in greatest use today are hard wired in a fixed location. This hard wiring is necessary to provide power for the terminal and to provide access to communication lines, such as telephone lines, over which data may be exchanged with the financial service provider. Security concerns also play a role in limiting ATMs to fixed locations.

As a result of the fixed location of such terminals, financial networks must take great care in distributing ATMs over a particular geographic region so as to maximize consumer access. However, with changing demographics, such distributions may become less advantageous. For example, a new shopping mall may open in a first location, increasing demand in that area, while another mall may close in a second location thereby decreasing demand in that location. One-time or isolated events resulting in an unexpected influx of people to a particular area may also result in an overwhelming demand which cannot be met satisfactorily by an existing distribution of terminals.

Currently, such problems may be addressed by providing additional ATM terminals. However, the capital costs of such terminals and the necessary peripheral equipment, such as power supplies, maintenance facilities and so forth may be too prohibitive to permit adaptive response to the above-described changes in consumer demand.

Accordingly, there is a need for a financial transaction and information system which can overcome the aforementioned shortcomings. Specifically, there is a need to provide transaction and information terminals which can be conveniently repositioned by the operator as necessary to maximize availability and use of the financial services provided thereby. Further, there is a need for transaction and information terminals which do not need to be directly connected by lines to a telephone network or power source network.

There is an additional need to provide the above-described features without compromising the security provided by existing systems and without introducing inordinate costs.

## SUMMARY OF THE INVENTION

It is an object of the invention to meet these needs, and others, through a financial information and transaction system which utilizes wireless communication in connection with portable terminals. In this system,

a terminal is connected to the financial institution via a wireless or cellular telephone hook-up. It is a feature of the invention that so-called "smart cards" are utilized to verify authorization for transactions, thereby minimizing potential security problems which could otherwise result from use of a mobile terminal. According to an alternate embodiment of the invention, a smart card is advantageously utilized not only for authorization, but also to maintain a secure record of available funds.

According to another embodiment of the invention, a portable transaction terminal is internally powered by, for example, rechargeable batteries. In an alternate embodiment, the terminal is powered by a standard ac power supply through a conventional outlet.

In yet another embodiment of the invention, a cellular telephone, having a smart card reader incorporated therein, is utilized as a data terminal for various financial transactions.

According to a further embodiment, the system not only provides the functionality of an ATM network, but also provides non-financial services thereby forming an integrated system.

The above, and other objects, features and advantages of the present invention will become readily apparent from the following detailed description thereof

which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

Fig. 1 is a block diagram of a financial information and transaction system in accordance with the invention.

Fig. 2A is a block diagram of a first application of the invention which includes a wireless transmitting/receiving station.

Fig. 2B is a block diagram showing a second application of the invention which includes a wireless transmission/receiving station.

Fig. 2C is a perspective view of a cellular telephone terminal in accordance with the invention.

Fig. 3A is a perspective/block view of a first portable wireless transaction and information terminal in accordance with the invention.

Fig. 3B is a perspective/block view of a second portable wireless transaction and information terminal in accordance with the invention.

Fig. 4 is a block diagram of a wireless transaction and information system in accordance with the invention.

Fig. 5 is a block diagram of a smart card according to the invention.

Fig. 6 is a block diagram of a file structure of the smart card of Fig. 5.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 is a block diagram illustrating a system for providing financial information and performing financial transactions in accordance with the present invention. In this embodiment, a financial institution is represented by block 10. As known in the art, the financial institution, such as a consumer banking institution, utilizes an automated system, including a host computer, for maintaining records of customer accounts. These records are used to keep track of funds in the customer accounts, to enter debits and credits made to such accounts, and for other purposes.

In order to provide various services to the customer, such as providing account information and account debiting and crediting at the customer's request, a communications front end 12 is used to exchange data corresponding to such information. The communication front end 12 provides access to the host computer operated by the financial institution 10 from a variety of communication systems. For example, as shown, the communications front end 12 may exchange data with a standard switch network 14, such as one operated by a regional telephone company. Thus, data transfer utilizing such a system generally takes place over the

telephone line. In this way, data may be exchanged with a user suitably linked to the standard switch network 14 with a modem using any of a variety of communication protocols known in the art. Moreover, data may be exchanged in this way other financial institutions and financial networks (not shown), for example, to provide data for settlement of various customer transactions.

Alternately, the communication front end 12 may be connected to a network service provider 16 or a private network 18. For example, one of several commercial services now available may link users throughout a geographic area. Further, the communications front end 12 may provide an interface between the financial institution 10 and a private network 18 comprising, for example, one or more local area networks (LAN) or wide area networks (WAN).

Further, the communications front end in this representation is connected to a direct wireless service 20. For example, such a hook-up could operate at a very high frequency (900 megahertz) along a cellular telephone-type or spread spectrum type connection (900 megahertz with multiplexers) for security purposes. The signal from the direct wireless service 20 may be received by a number of different types of terminals, described below.

As illustrated, Fig. 1 shows direct links between the communications front end 12 and the various

types of communication systems 14, 16, 18, and 20. However, it will be understood by those skilled in the art that various combinations of such systems, and others, are possible. For example, a private network 22 may be accessed with the communications front end 12 through a network service provider 16. Alternatively, rather than the direct wireless communication represented by block 20, wireless communication may take place using various commercial wireless service providers 24 via the standard switch network 14. Other networks 26, such as the so-called "Internet," may be accessed with the standard switch networks 14.

Figs. 2A to 2C illustrate various applications in which wireless data transmission may be utilized to provide convenient access to a financial institution, such as the financial institution 10 mentioned above in relation to Fig. 1. For example, Fig. 2A illustrates an application in which a wireless transmitting and receiving station 50 is operatively linked to various terminals A to D distributed in a shopping mall 52 or other localized area.

In Fig. 2B, a wireless transmitting and receiving station 54 is operatively linked to a financial server 56 associated with LAN or WAN of a business. Various nodes 58, 60, and 64 are provided along the network of the business. One such node 64

shown in Fig. 2B may comprise a personal computer which includes a smart card reader 64a.

In Fig. 2C a cellular telephone 75 serves as a financial information and transaction terminal. In this embodiment, the cellular telephone 75 includes standard features such as an alpha-numerical keypad 80, a speaker portion 76, a microphone portion 82, and a display 78 (for example, a LCD display). Additionally, a smart card reader portion 84 is provided. This additional feature provides the additional capability to perform financial transactions using the keypad 80 as an interface. The functionality of this embodiment and of those described above is apparent from the ensuing description.

Figs. 3A and 3B illustrate in greater detail embodiments of a portable, wireless terminal in accordance with the invention. In both of these embodiments and in those which are later described, use is made of a smart card and a smart card reader. As is known in the art, a smart card is a device which may include processing means as well as both volatile and non-volatile memory. Data stored in read-write memory on the smart card may be exchanged with a reader device, typically through a serial interface. One advantage of such use of the smart card is that encryption algorithms may be stored and processed with the smart card to allow the smart card to be validated from a remote location, for example, by a host computer operated by a financial

institution. In this way, information can be securely exchanged between the card and the remote location using one or more encryption keys that are in place in both locations. The encryption keys are used to encode information to be transmitted and to decode information that is received.

Using encryption techniques, it is possible not only to encode financial information stored remotely by a host computer or locally on the smart card, but also to encode identification information, such as personal identification numbers (PINs). In this way a user's PIN may be encrypted by the smart card and communicated to a remote host which has the same encryption key to decode the encrypted PIN and to validate it. This provides authorization to access information stored by the host and/or to request various financial transactions.

Fig. 3A illustrates a first wireless terminal 100 for use with a smart card. This terminal 100 includes a customer interface 102, such as an alpha-numerical keypad 104, a display 106, and a smart card reader 108. Signals provided from a wireless service provider, such as one described in Fig. 1, are received by a transmitter/receiver portion 110 of the terminal 100. Conversely, signals are provided from the transmitter/receiver portion 110 of the terminal 100 to a front end processor via wireless service provider. In this manner, the terminal 100 may be used to wirelessly

receive and transmit data to and from a financial institution or financial network. This data may then be read and write from and onto a smart card that is inserted into the smart card reader 108.

In this embodiment, the terminal 100 may be advantageously used to read data stored on a smart card to determine, for example, a value corresponding to an amount of funds existing in the user's account. With the terminal 100, the user may add to the amount stored on the card and have the added amount debited from the user's account by the host computer. In such a way, the terminal thereby functions as a credit-authorization terminal. The authorization and financial information is kept secure during transmission as a result of the encryption capabilities of a smart card that is used to access the terminal 100.

For example, the user may insert a smart card into the smart card reader 108. The card first encrypts, then transmits to the terminal 100 information stored on a smart card. This information identifies the financial institution which maintains the user's account as well as the user's account number. Additional security may be obtained by requiring that the user input a PIN with the numeric keypad. Again, the smart card can then encrypt the PIN for transmission by the terminal to a host computer for verification.

Once authorization has been obtained, the user may determine the user's current account balance and/or request that value be added to the card. In executing these requests, the terminal exchanges encoded information by wireless transmission with a financial network, such as one described above with respect to Fig. 1. For example, the terminal may be used to directly add value to the user's card, and then request by wireless transmission that the customer's account be debited a corresponding amount. These requests comprise encoded data which is decoded by the host computer associated with financial institution.

When the funds are transferred to and from the smart card, an encrypted bank signature appended to the funds certifies that the funds are "real." It also ensures that when the transaction enters the settlement system, the funds are validated. Because the settlement system may involve more than one financial institution, when the transaction is ultimately presented to the financial institution for payment, the encrypted bank signature verifies that the transaction is authentic.

In the embodiment shown in Fig. 3A, the terminal 100 may operate with a standard ac supply 112 from a conventional outlet. In the embodiment of Fig. 3B (in which identical reference numerals are used to refer to corresponding structure described in reference to Fig.

3A), a terminal 120 is powered by rechargeable batteries 122 in order to provide even greater mobility.

It will be appreciated that such a terminal as described in reference to Figs. 3A and 3B permits the user to conduct numerous financial transactions without a hard wired connection between the terminal and the financial institution. For example, the terminal can be used to "recharge" a smart card in the manner described above. After "recharging," the user may then use the card in connection with terminals that accept this "electronic cash" in lieu of cash by deducting an amount from the user's card. The amount deducted can then be redeemed by a merchant through a settlement process with the user's financial institution (and others).

It can be seen that the terminal described in Figs. 3A and 3B is a truly mobile unit and enjoys the benefits of such mobility. Because the terminal is not required to dispense cash, no safe is required. This, in turn, reduces the cost and size of the terminal and maximizes the flexibility of the design of the terminal. For example, the terminal may be positioned in the corridor of a mall or an office building, thereby maximizing its access and availability to foot traffic during the day. At night, the terminal could be rolled back in from the corridor and accessed for settlement/verification procedures in accordance with standard industry practice with ATMs. In the embodiment

of Fig. 3B, the terminal's batteries could be recharged during this time for use the next day.

Alternatively, the mobile terminal could be positioned on a truck which could be parked outside at a fair or sporting event and powered by batteries or a generator stored on the truck. Again, the mobile terminal is positioned to maximize access to foot traffic and is repositioned at night for recharging, servicing, etc. Positioned in this way, the above-described terminals provide increased flexibility and adaptiveness for responding to customer demands.

Fig. 4 illustrates another embodiment of the invention in which a wireless server/terminal unit 150 is used to exchange financial information between a user and a remote host computer of a financial institution, such as that referred to in Fig. 1. The wireless server/terminal unit 150 preferably includes a terminal described above in reference to Figs. 3A and 3B (that is, one which incorporates a display, a keypad, a smart card reader, and means for wireless transmission of data).

The system shown in Fig. 4 integrates the capability of exchanging financial information with other non-financial functionality, such as security control. In particular, the wireless server/terminal unit 150 forms a portion of a LAN which comprises a variety of other computers and networks. As illustrated, these other computers and networks include an employee's work

place PC 158, an employee's home PC 152, a WAN 156, a local building computer system 154, a conventional ATM 160, and a spread spectrum server 162.

A variety of terminals and associate device are coupled to the networks shown. For example, the WAN 156 includes PCs 166 and 168. A building access system 174 includes various smart card readers 170, some of which are equipped with keypads. Similarly, each of the employee PCs 152 and 158 are equipped with smart card readers 152a and 158a.

Also, a plurality of terminals, represented by the terminal 172, are coupled to the spread spectrum server 162. For example, the terminal 172 is equipped with a smart card reader 172a. In this way, the wireless financial server terminal 150 enables employees to access their financial institution through a variety of means and from a variety of locations in the work place and at home.

In particular, the wireless smart card recharge station 172 communicates to the financial institution via the spread spectrum receiver 162 and the server terminal 150. The recharge station 172 has a slot for receiving and reading a smart card and a display (see Figs. 3A and 3B). Through its connection with a financial system, such as that shown in Fig. 1, the user makes selections from a menu displayed on the display of the terminal 172. For example, the user may review account balances,

transfer funds, or perform other activities typically available on a fixed-location ATM. The user may also reload monetary value onto the smart card via the cash station, adding set funds to either a "prepaid" or "purse" account on the smart card as described below. In this way the user can obtain access to money via a portable ATM-type terminal without security risk because no cash is directly involved. At the end of the user's visit to a location where the smart card is honored, the user may employ the station to deposit any unused balances from the user's smart card to the user's account with the financial institution.

As shown, a user's PC 152 may be connected to a smart card reader, such as one having a keypad and processing capabilities. This enables the user to access the user's financial accounts and to "recharge" the smart card (that is, add funds onto the smart card). In this respect, the keypad enables the user to enter the user's PIN and the smart card inserted into reader 152a provides additional encryption and security measures to make the transport route (namely, the LAN/wireless terminal/route) sufficiently secure to conduct financial transactions. A similar arrangement is conducted at other remote locations through a telephone line connection between the terminal and the employee's home personal computer connected to a smart card reader/processor and keypad. Further, a smart card reader/processor with a display

which simulates an ATM protocol could be connected to the terminal, thereby enabling the user to perform all ATM functions including recharging the smart card, without the use of a personal computer.

Thus, the server terminal 150 provides a communications channel for several remote devices, such as the home PC 152, the work place PC 158 and the terminals 172 associated with the spread spectrum server 162 and those associated with the wide area network 156. By providing card readers with these terminals, it is possible to obtain a wide range of access points to a remote host computer via the wireless financial server/terminal. This provides additional capabilities to the above-described financial information and transactions.

Additionally, the embodiment of Fig. 4 describes an integrated system which may be used for other non-financial transactions. For example, the building computer system 154 noted above may be used to control a building access system 174. The building access system of this example includes a plurality of smart card readers and/or keypads. Such interface devices may be used to verify that a user is authorized to enter particular areas by matching information stored on a smart card against security records maintained or updated through the server/terminal unit 150. Different security levels may be instituted for different areas,

each requiring additional authorization. For example, it may only be necessary to insert a card to access a parking garage, while gaining access to particular rooms may require additional authorization, for example, the inputting of a PIN with a keypad.

Fig. 5 illustrates a multi-purpose smart card 200 which permits both financial and non-financial functions in an integrated system such as that described in Fig. 4. The smart card 200 comprises a central processing unit 202 (CPU) which is connected to a read only memory 204(ROM), primarily used for storage of an operating system. A random access memory 206 (RAM) is also provided for volatile storage of data, particularly for program execution. The CPU 202 is operatively coupled to a serial interface 208 which in turn communicates with a smart card reader 210 according to techniques well known in the art.

The CPU is connected to an arithmetic logic unit 212, for example, one suitable for processing large keys (512 byte keys). An electrically erasable programmable read only memory 214 (EEPROM) is provided, which typically stores system files and applications.

As illustrated in Fig. 6, the smart card 200 of Fig. 5 has different file paths for different functions. The EEPROM has a master file 220 and dedicated files for different applications. These dedicated files include a biometric identification file 222 and an encrypted

digital signature file 224. Also included is a building access file 226 that contains information which enables the card to be used in conjunction with a security system, such as the one referred to in Fig. 4. The master file 220 also is linked to a banking card debit file 228 which may also have its own security path for identification. The smart card has a prepaid function path 230 which can only be loaded through a secure function, and a "non-secure" electronic purse function file 232. These files are readable by an external terminal, such as the terminal described in reference to Figs. 3A and 3B, and may be decremented as required from an outside terminal, as described more fully below.

In this example, the master file 220 also has a digital encryption capability 234 providing algorithmic computation for the processing of digital keys and encryption of, for example, the user's PIN. The algorithms used may provide symmetrical or asymmetrical encryption as known in the art.

While the smart card utilized in the invention embodies a "computer", it has a fairly limited memory. For example, the EEPROM may be limited to the range between 3 to 8 kilobytes with current technology limitations. Accordingly, the smart card in the system preferably acts as an enabling device for other systems according to known techniques. For example, the smart card provides validation of the individual and the

service requested, but does not store large quantities of data on the card.

It should be understood from the above description that as the mobility of an ATM-type terminal increases, security concerns may also increase. More specifically, it may be unfeasible to place cash in a mobile ATM due to the possibility of theft of the terminal. Use of a smart card enables the system to provide users with secure purchasing in a cash-free environment.

Further addressing this concern, the smart card 200 of Figs. 5 and 6 includes two storage areas for storing monetary values. The first is an "electronic purse" represented by file 232. This area is used, for example, when the user makes a high value purchase by placing the smart card in a merchant's terminal. The user accepts the transaction and amount of the purchase entered by the merchant by entering the user's PIN. The user then approves the amount, for example, by pushing an "enter" button on a terminal keypad, the card purse cash value is then debited by the requested amount, and, conversely, the merchant's account is credited that amount.

A second area for storing monetary values on the card comprises a "pre-paid account" represented by file 230. This account is generally utilized for lower value purchases, for example, fifty dollars or less.

This account is kept in an unsecured cash area of the smart card and operates essentially like cash. For example, the user of the smart card may make purchases from this account without entering the user's PIN. Possible uses would include, preferably, low value, fast transactions such as at a cafeteria, or a vending machine, or when placing a local telephone call.

The smart cards referred herein interface with the system through the use of various smart card reader/processors. These processors vary in complexity and sophistication depending upon the application. For example, when used to regulate building access, the smart card may be inserted into a smart card reader which simply identifies the user. This could be used in lower security areas, such as parking garages. A numerical keypad, by which a user's PIN may be entered, can be required for added security, such as at building door entrances. For even further security, some biometric parameter (such as a fingerprint) may be used for identification. This same access code with or without a PIN can be used in a smart card reader attached to a stand-alone or network personal computer 158A to control the level of access to local or remote files, communication networks, databases and network services.

In the aforementioned embodiments, the smart card incorporates optional digital encryption signatures and encryption algorithms to enable the smart card to be

validated from a remote location, such as a host computer at a financial institution or at off/on line merchant terminals equipped with a SAM module for off-line card authentication. In such instances both ends of the communication (for example, the host computer and the smart card) may each have an encryption key so that data (such as a PIN entry) which is sent via the smart card 60 is validated at the host computer. Thus, the host computer is able to validate that the smart card is authentic and that the proper user is using the smart card so that a financial transaction can take place.

In a wireless off-line situation, the smart card and the terminal being used similarly validate one another because there is a possibility that a false terminal is being used. Accordingly, even in an off line system, security measures are available to validate the card, the terminal, and the user.

Various preferred embodiments of the invention have now been described in fulfillment of the objects of the invention. While these embodiments have been set forth by way of example, various other embodiments and modifications will be apparent to those skilled in the art. Accordingly, it should be understood that the invention is not limited to such embodiments, but encompasses all that which is described in the following claims.

WHAT IS CLAIMED IS:

1. A financial information and transaction system comprising:

a host financial computer system, said host system maintaining records of user account information;

at least one terminal providing a user interface for accessing said host financial computer system, said at least one terminal including first means for wirelessly transmitting and receiving data, and a smart card reader; and

communication means for operatively coupling said terminal to said host system whereby data corresponding to said user account information is exchanged between said at least one terminal and said host system, said communication means including second means for wirelessly transmitting and receiving data with said first means for wirelessly transmitting and receiving data;

wherein a user accesses said host financial system through a smart card device that is coupled to said smart card reader, said smart card device including means for encrypting data which is exchanged with said host financial system.

2. The financial information and transaction system according to claim 1, wherein said communication

means comprises means for transmitting and receiving data at a frequency of about 900 megahertz or more.

3. The financial information and transaction system according to claim 1, wherein said at least one terminal comprises a plurality of terminal devices coupled to a common wireless transmitting and receiving station.

4. The financial information and transaction system according to claim 1, wherein said plurality of terminals are arranged in a local area network.

5. The financial information and transaction system according to claim 1, wherein said at least one terminal comprises a wireless cellular telephone device.

6. The financial information and transaction system according to claim 5, wherein said wireless cellular telephone device includes a smart card reader incorporated therein.

7. The financial information and transaction system according to claim 1, wherein said at least one terminal comprises a portable terminal that includes a keypad and display.

8. The financial information and transaction system according to claim 7, wherein said portable terminal is supplied with ac power from a standard power supply.

9. The financial information and transaction system according to claim 7, wherein said portable terminal is battery operated.

10. The financial information and transaction system according to claim 4, wherein local area network includes a plurality of personal computers, each having smart card readers by which a user may encrypt and decode data which is exchanged with said host system.

11. The financial information and transaction system according to claim 1, wherein said at least one terminal is operatively coupled to a security system for controlling access to various physical locations each associated with a smart card reader, said security system providing access to said various locations by matching information stored on a user smart card which is inserted into said associated smart card readers.

12. The financial information and transaction system according to claim 1, wherein said smart card device includes a plurality of files stored therein.

13. The financial information and transaction system according to claim 12, wherein one of said plurality of files corresponds to an encryption key which is executed by processing means provided in said smart card device, thereby encrypting data provided to said smart card device.

14. The financial information and transaction system according to claim 12, wherein one of said plurality of files is a banking card debit file, said banking card debit file containing data elements for execution of a debiting of said user account.

15. The financial information and transaction system according to claim 12, wherein one of said plurality of files is an electronic prepaid function file, said electronic prepaid function file maintaining data elements representative of a monetary value which is augmented or decremented by said at least one terminal upon authorization by the user.

16. The financial information and transaction system according to claim 15, wherein said authorization is obtained by the user inputting a personal identification number associated with the user's account.

17. The financial information and transaction system according to claim 13, wherein one of said plurality of files is an electronic purse function file, said electronic purse function file maintaining data elements representative of a monetary value which is augmented or decremented by said at least one terminal.

18. The financial information and transaction system according to claim 1, wherein said at least one terminal is coupled to a security system for controlling access to various physical locations each associated with a smart card reader, wherein said smart card device includes at least one file containing data elements for providing authorization to access one or more of said physical locations.

19. The financial information and transaction system according to claim 18, wherein said smart card device includes a biometric identification file which contains identification data corresponding to unique physical characteristics of a user, said identification data being used to authorize access to one or more of said physical locations.

20. The financial information and transaction system according to claim 18, wherein said authorization to access said one or more physical locations is obtained

by the user inputting a personal identification number associated with the user.

21. The financial information and transaction system according to claim 1, wherein said at least one terminal is coupled to a host system for controlling access to a communication network and wherein said smart card device includes at least one file containing data elements for providing authorization to access said communication network.

22. The financial information and transaction system according to claim 1, wherein said at least one terminal is coupled to a host system for controlling access to a network device and wherein said smart card device includes at least one file containing data elements for providing authorization to access said network service.

23. The financial information and transaction system according to claim 1, wherein said at least one terminal is coupled to a host system for controlling access to a data base and wherein said smart card device includes at least one file containing data elements for providing authorization to access said data base.

24. The financial institution and transaction system according to claim 21, wherein said smart card device includes a biometric identification file which contains identification data corresponding to unique physical characteristics of said user, said identification data being used to authorize access to said communication network.

25. The financial institution and transaction system according to claim 22, wherein said smart card device includes a biometric identification file which contains identification data corresponding to unique physical characteristics of said user, said identification data being used to authorize access to said network service.

26. The financial institution and transaction system according to claim 23, wherein said smart card device includes a biometric identification file which contains identification data corresponding to unique physical characteristics of said user, said identification data being used to authorize access to said data base.

27. The financial information and transaction system according to claim 21, wherein said authorization to access said communication network is obtained by the

user inputting a personal identification number associated with the user.

28. The financial information and transaction system according to claim 22, wherein said authorization to access said network service is obtained by the user inputting a personal identification number associated with the user.

29. The financial information and transaction system according to claim 23, wherein said authorization to access said data base is obtained by the user inputting a personal identification number associated with the user.

30. The financial information and transaction system according to claim 1, wherein said plurality of terminals are arranged as part of a wide area network.

FIG. 1

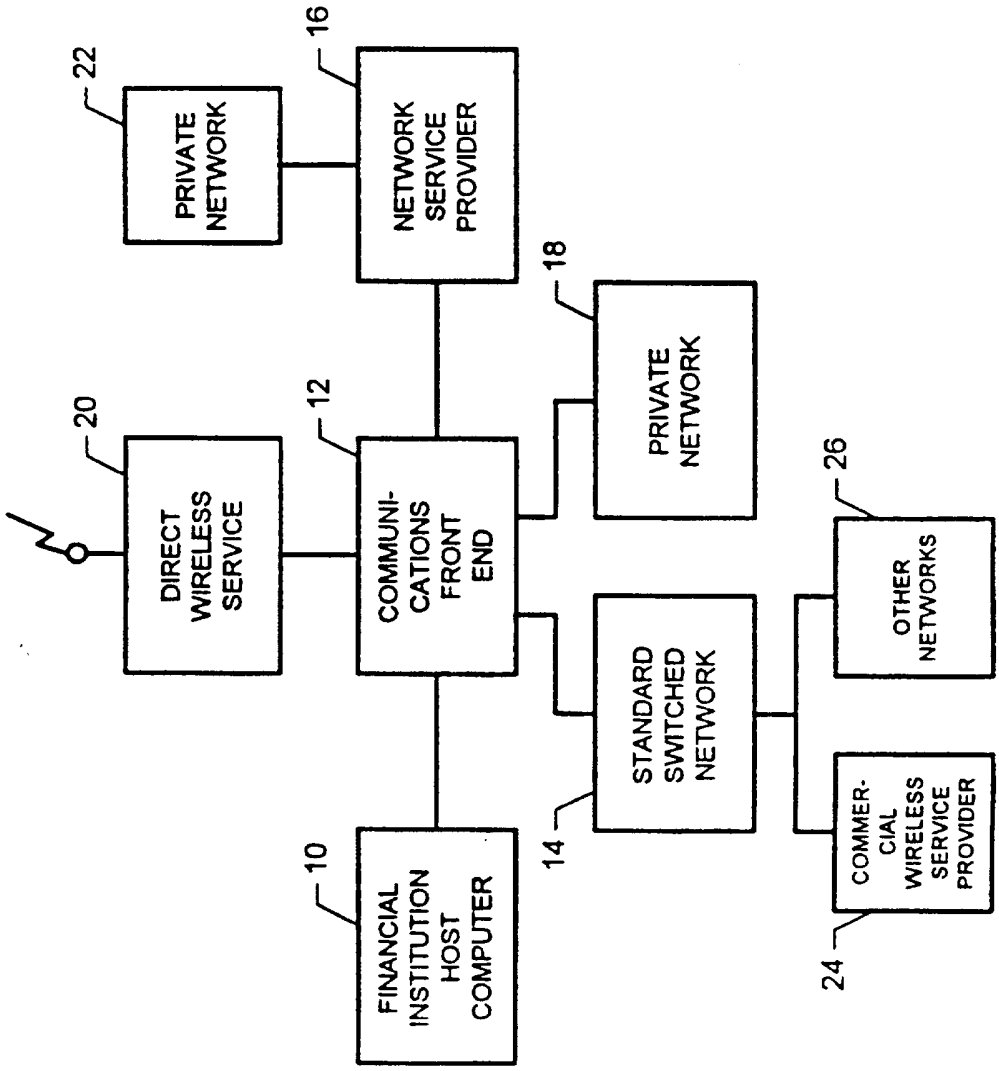

22
PRIVATE NETWORK
16
NETWORK SERVICE PROVIDER
18
PRIVATE NETWORK
20
DIRECT WIRELESS SERVICE
12
COMMUNI-CATIONS FRONT END
26
OTHER NETWORKS
STANDARD SWITCHED NETWORK
14
COMMER-CIAL WIRELESS SERVICE PROVIDER
24
10
FINANCIAL INSTITUTION HOST COMPUTER

FIG. 2A

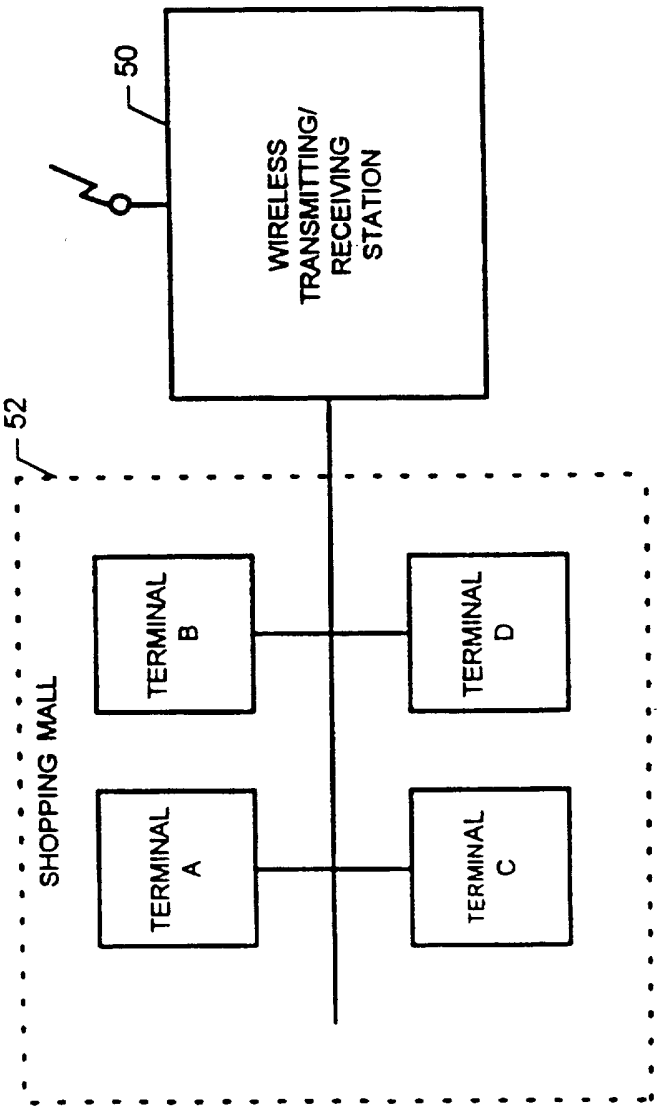

50
WIRELESS TRANSMITTING/ RECEIVING STATION
52
SHOPPING MALL
TERMINAL A
TERMINAL B
TERMINAL C
TERMINAL D

FIG. 2B

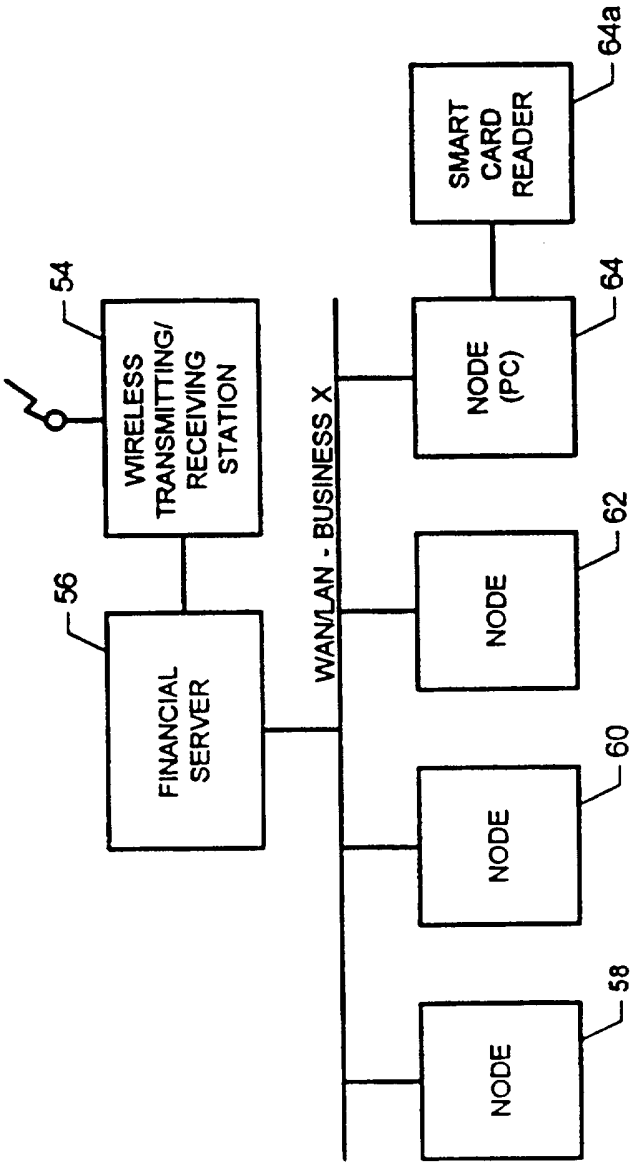

54
WIRELESS TRANSMITTING/ RECEIVING STATION
56
FINANCIAL SERVER
WAN/LAN - BUSINESS X
64a
SMART CARD READER
64
NODE (PC)
62
NODE
60
NODE
58
NODE

FIG. 2C

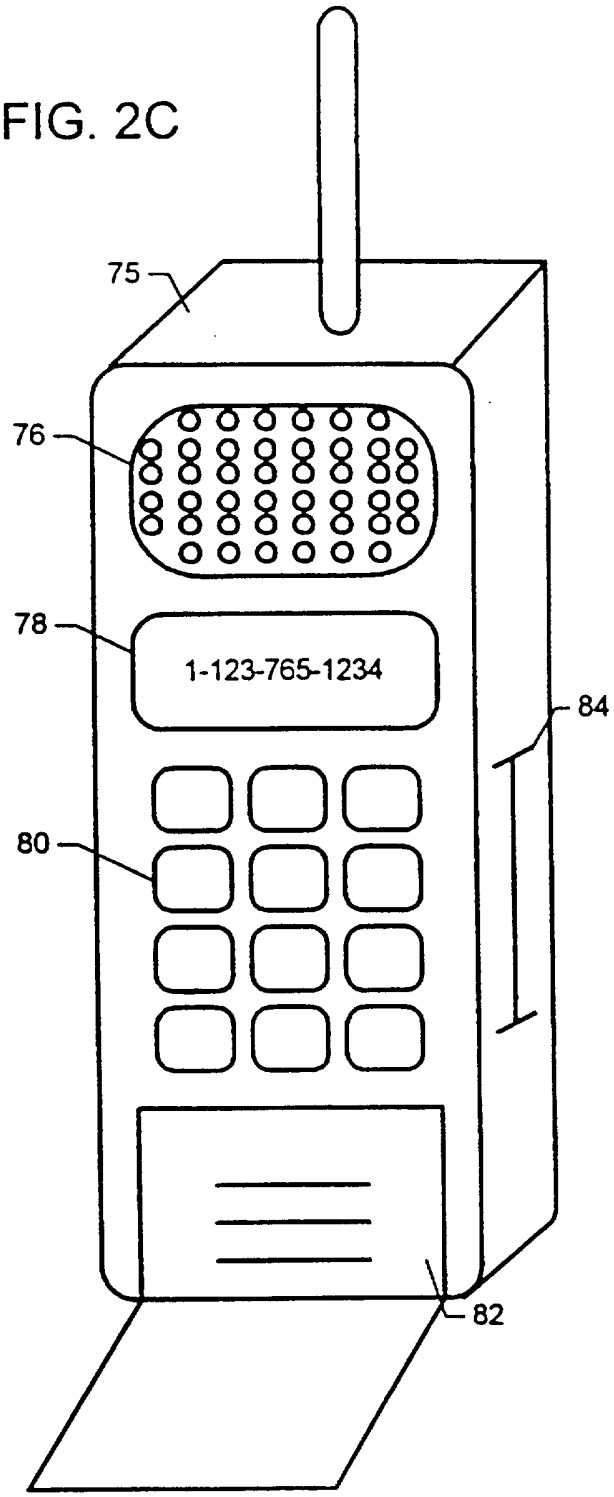


FIG. 3A

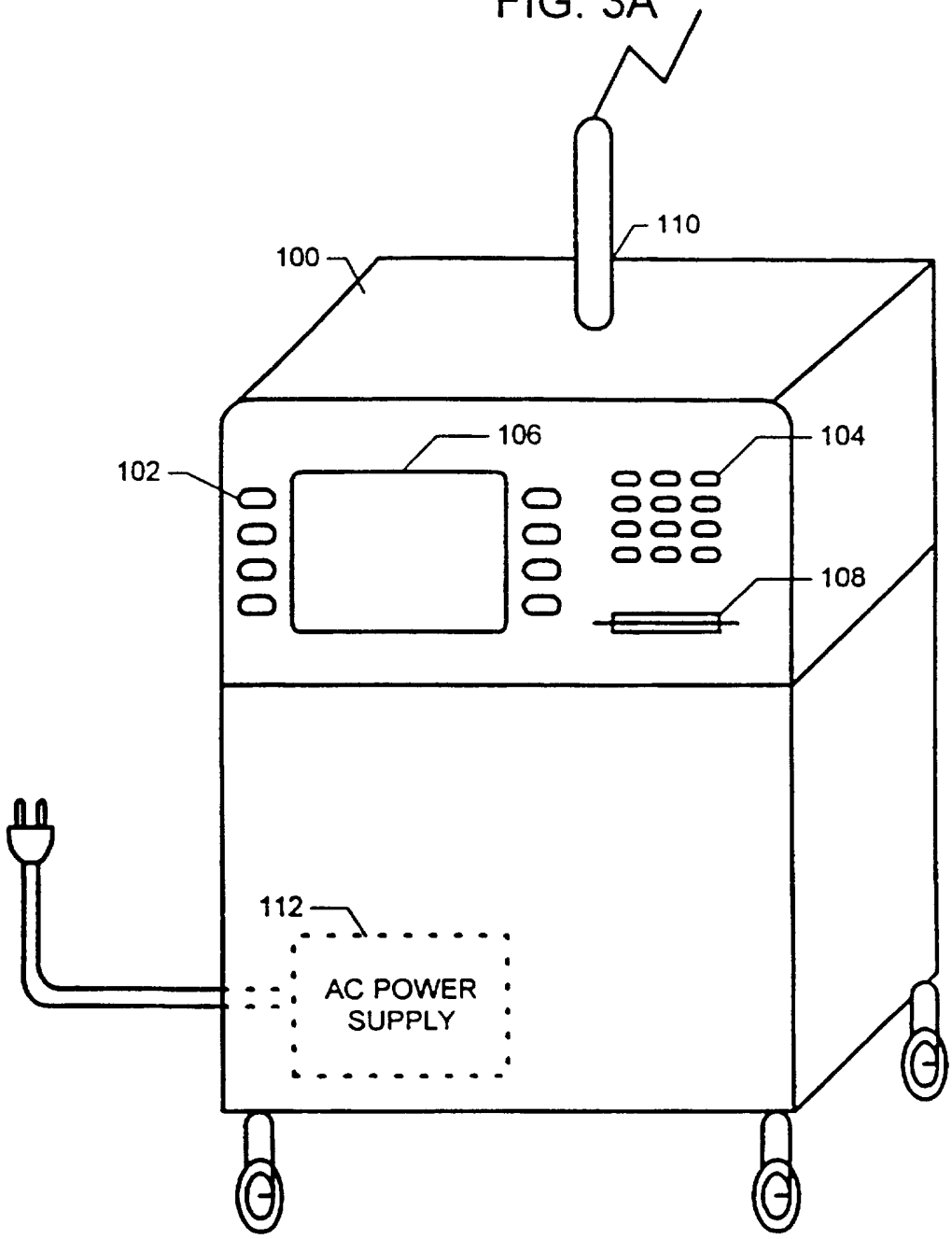


FIG. 3B

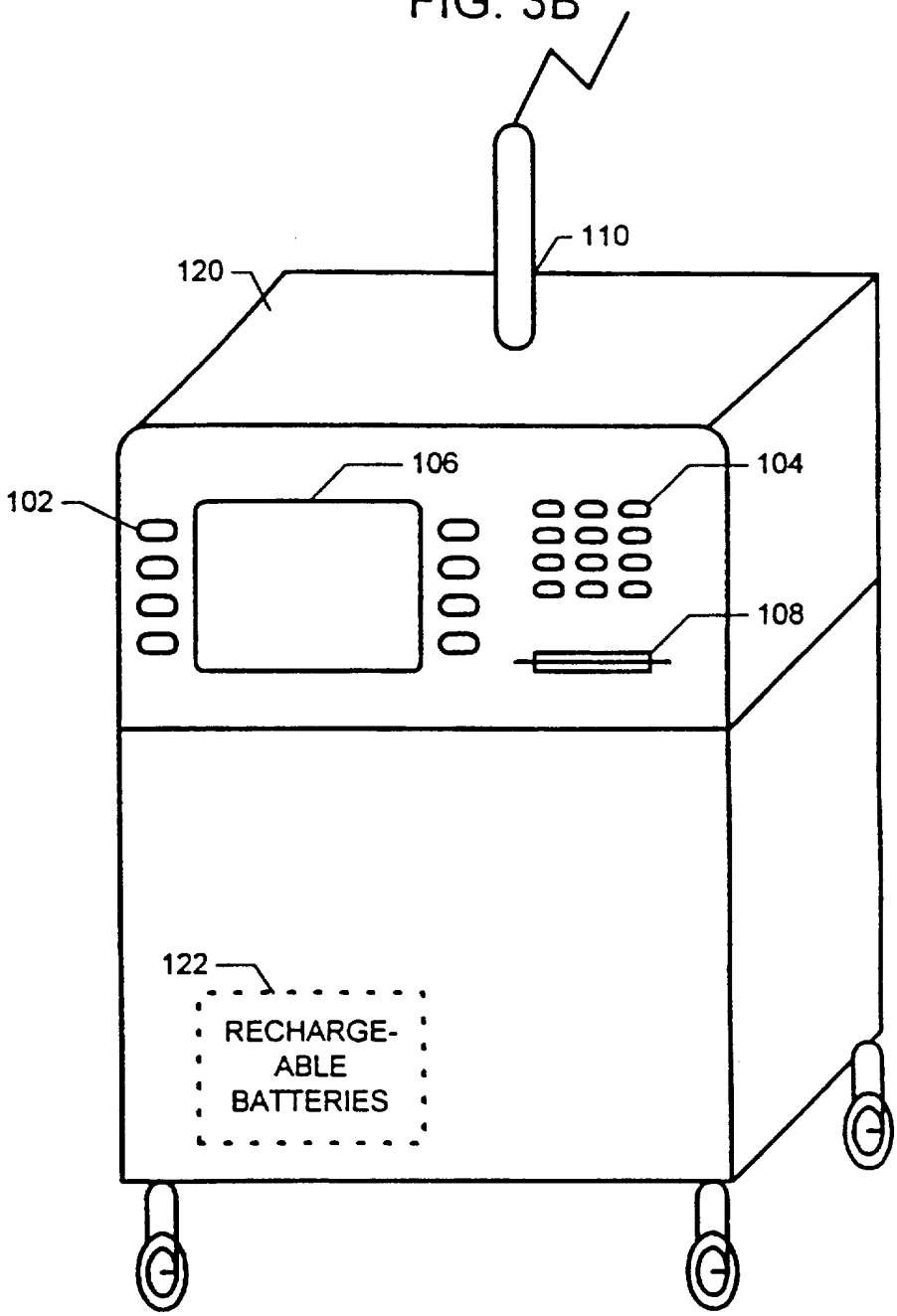


FIG. 4

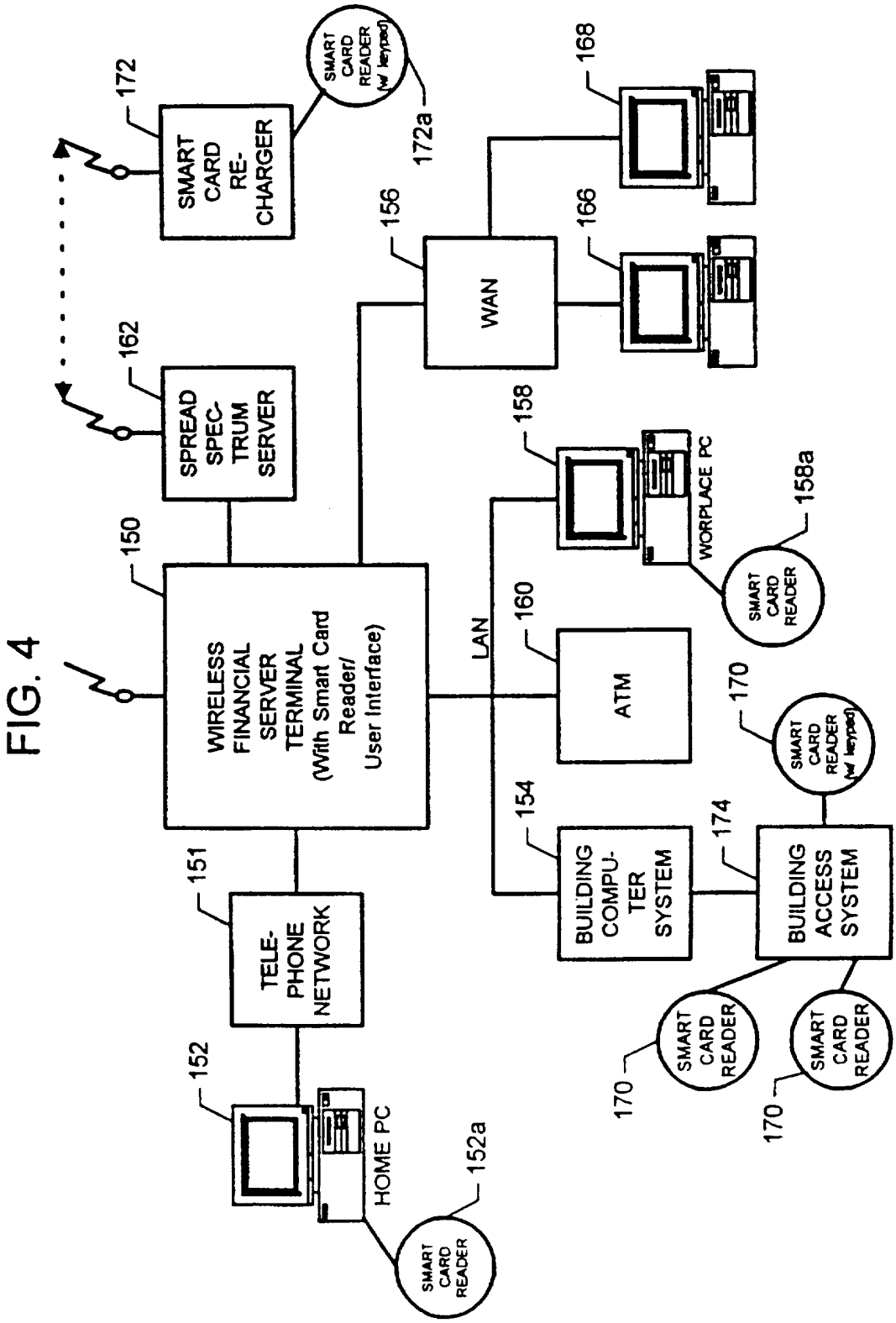

WIRELESS FINANCIAL SERVER TERMINAL (With Smart Card Reader/ User Interface)
150
SMART CARD RE-CHARGER
172
SMART CARD READER (w/ keypad)
172a
SPREAD SPEC-TRUM SERVER
162
WAN
156
168
166
158
WORKPLACE PC
158a
SMART CARD READER
LAN
160
ATM
170
SMART CARD READER (w/ keypad)
154
BUILDING COMPU-TER SYSTEM
174
BUILDING ACCESS SYSTEM
TELE-PHONE NETWORK
151
152
HOME PC
152a
SMART CARD READER
SMART CARD READER
SMART CARD READER

FIG. 5

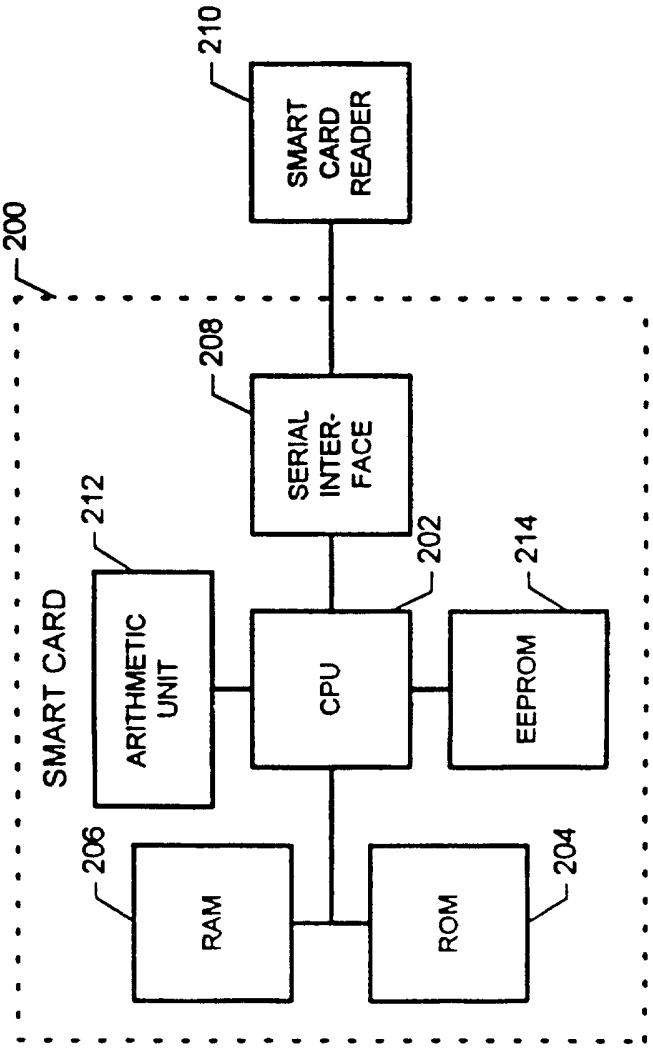
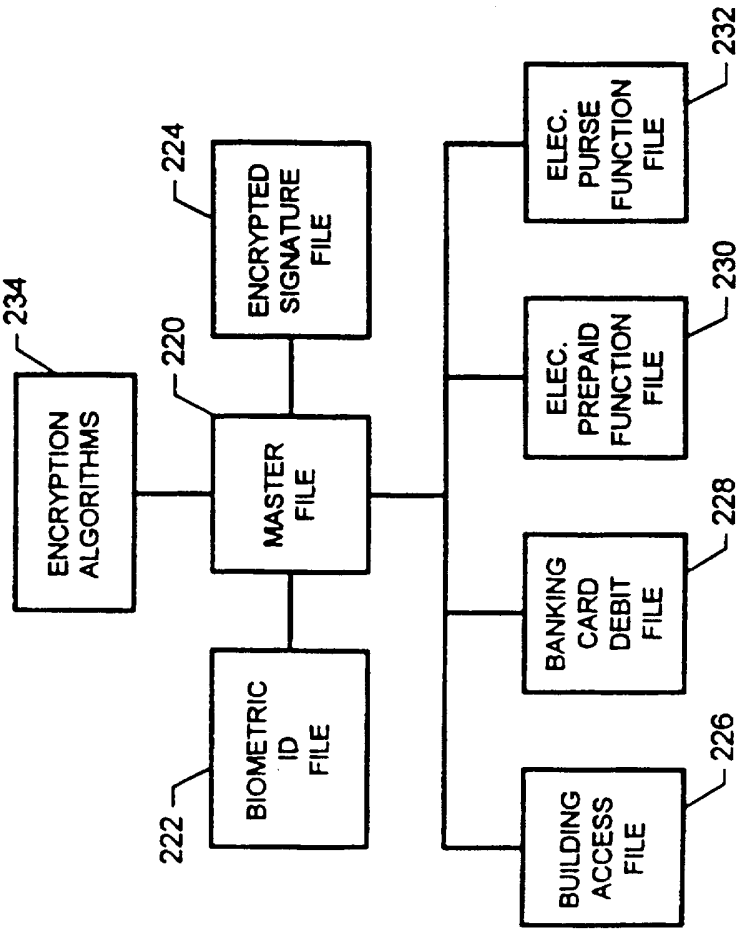

210
SMART CARD READER
200
208
SERIAL INTER-FACE
212
SMART CARD
ARITHMETIC UNIT
CPU
202
214
EEPROM
206
RAM
ROM
204

FIG. 6


ENCRYPTION ALGORITHMS
234
MASTER FILE
220
BIOMETRIC ID FILE
222
ENCRYPTED SIGNATURE FILE
224
BUILDING ACCESS FILE
226
BANKING CARD DEBIT FILE
228
ELEC. PREPAID FUNCTION FILE
230
ELEC. PURSE FUNCTION FILE
232

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/17902

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/25

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. : 380/24, 25; 235/380

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. |
|---|---|---|
| Y | US, A, 5,221,838 (GUTMAN ET AL) 22 June 1993, see Fig. 3. | 1-30 |
| Y | US, A, 5,461,217 (CLAUS) 24 October 1995, see Figs. 1-2. | 1-30 |
| Y | US, A, 5,341,428 (SCHATZ) 23 August 1994, see col. 3, lines 30-45. | 1-30 |
| . | . | . |
| . | . | . |
| . | . | . |

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

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "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 |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "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 |
| "E" | earlier document published on or after the international filing date | "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 |
| "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) | "&" | document member of the same patent family |
| "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 | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>26 FEBRUARY 1997 | Date of mailing of the international search report<br>26 MAR 1997 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>SALVATORE CANGIALOSI<br>Telephone No. (703) 305-1837 |

Form PCT/ISA/210 (second sheet)(July 1992)*