PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04K — A2

(11) International Publication Number: WO 00/52866

(43) International Publication Date: 8 September 2000 (08.09.00)

(21) International Application Number: PCT/US00/04819

(22) International Filing Date: 25 February 2000 (25.02.00)

(30) Priority Data:
09/260,384 — 2 March 1999 (02.03.99) — US

(71) Applicant: ESIGN, INC. [US/US]; 50 Airport Parkway, San Jose, CA 95110 (US).

(72) Inventor: WANG, Yujiun; 50 Airport Parkway, San Jose, CA 95110 (US).

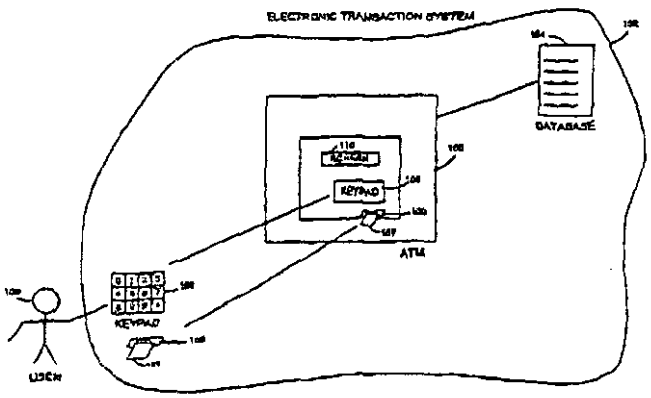
(74) Agents: ASHBY, David, C. et al.; Flehr, Hohbach, Test, Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111-4187 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: PORTABLE ELECTRONIC CHARGE AND AUTHORIZATION DEVICES AND METHODS THEREFOR



(57) Abstract

A portable transaction arrangement for permitting a user to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system. The charge card terminal is configured to communicate with a charge card for the purpose of conducting the charge card transaction. The charge card is one of a magnetic stripe card and an electronic smart card. The portable transaction arrangement includes an emulation card having an emulation card interface. The emulation card interface emulates an interface of the charge card. The interface of the charge card facilitates communication between the charge card and the charge card terminal. There is also included a portable emulation card configuring device arranged to be used in conjunction with the emulation card, which in turn includes a memory configured to store first charge card data pertaining to a first charge card of the user, and an authentication mechanism. The portable emulation card configuring device is configured to write from the memory the first charge card data to the emulation card if the user is authenticated through the authentication mechanism, thereby allowing the emulation card to appear through the emulation card interface, after writing and for the purpose of conducting the transaction, like the first charge card to the charge card terminal and enabling the charge card terminal to read the first charge card data from the emulation card to conduct the charge card transaction.

PORTABLE ELECTRONIC CHARGE AND AUTHORIZATION DEVICES AND METHODS THEREFOR

Background of the Invention

The present invention relates to methods and apparatus for conducting electronic transactions. More particularly, the present invention relates to portable electronic authorization devices (PEADs) which advantageously and substantially eliminate the security risks associated with prior art techniques of approving transactions between a user and an electronic transaction system.

Electronic transaction systems are known. An electronic transaction system typically permits a user to conduct designated transactions electronically, which substantially improves efficiency and convenience to the user. Examples of electronic transactions include transactions conducted via computer networks, automated teller machines (ATM's), automated point-of-sale systems, automated library systems, and the like. Transactions conducted via computer networks may encompass a wide range of transactions, including exchanging information and data via a computer network popularly known as the Internet, e.g., to make a purchase from a vendor on the network. ATM's typically permit users to conduct financial transactions (such as withdrawals, transfers, deposits, and the like) vis-à-vis a financial institution in an electronic manner. Automated point-of-sale systems may be employed by merchants to

permit users to purchase products or services using the users' electronic account, and automated library systems may be employed to permit library users to check out and return library materials. Other examples of electronic transaction systems are readily available in popular literature and are not enumerated herein for brevity sake.

To enhance security to the user's account, electronic transaction systems typically request the user to provide identification data to authenticate himself as the user authorized to approve the proposed transaction or transactions. If the user fails to provide the requested identification data, the proposed transaction or transactions are not authorized and will not be processed. The identification data may be required with each transaction. By way of example, an automated point-of-sale system may require the user to approve a purchase transaction and will accept an approval message only if it is satisfied that the person approving the transaction has furnished adequate identifying data authenticating himself as the person authorized to perform the approval. Alternatively, the identification data may be entered by the user at the start of a session to authenticate himself and enable that user to subsequently perform any number of transactions without further authentication.

In the prior art, users are typically required to manually enter the identification data into the electronic transaction system for authentication. Typically, the entry of identification data involves typing in a password on a numeric keypad or on a keyboard. The identification data is then compared with data previously stored within the electronic transaction system, and authentication is satisfied when there is a match. As mentioned previously, the transaction or transactions proposed will not be allowed to proceed if there is no match.

Although prior art electronic transaction systems provide some protection from unauthorized access and use of the user's account, there are disadvantages. To illustrate certain disadvantages associated with prior art

electronic transaction systems, reference may be made to Fig. 1 herein. Fig. 1 shows an automated teller machine (ATM) 100, representing the requesting device of an electronic transaction system 102. Electronic transaction system 102 may include, for example, a central database 104 which contains previously-stored identification data and account data of user 106.

To initiate a typical transaction with ATM 100, user 106 first inserts a data card 107, such as a bank card or a credit card, into a card reader 109. Data card 107 typically includes a magnetic stripe that contains the account number and other information related to the user, which may then be read by card reader 109. The data stored in data card 107 enables electronic transaction system 102 to ascertain which account in database 104 user 106 wishes to transact business.

Via a keypad 108 on ATM 100, user 106 may then be able to enter his identification data, e.g., his personal identification number (PIN), to authenticate himself. If the entered identification data matches the identification data stored with the account in database 104 that is identified by data card 107, the user is authenticated and granted access to his account. If there is no match, authentication fails. After authentication, user 106 may be able to, for example, employ a combination of keypad 108 and a screen 110 to withdraw cash from his account, which results in cash being dispensed from ATM 100 and the balance in his account within database 104 correspondingly reduced.

Theoretically, the identification data entered into ATM 100 should be secure. In reality, there are many potential security risks to the identification data in prior art authentication techniques. Since the identification data is not encrypted before being entered into ATM 100, the non-encrypted identification data is vulnerable to unauthorized access and procurement. Encryption of the identification data is not practical in the prior art since it would have been too complicated and/or inconvenient for the user to perform encryption or memorize the encrypted identification data. Unauthorized

procurement of the identification data in the prior art may occur, for example, upon entry if it is inadvertently seen by another party, e.g., by another person behind user 106, either on screen 110 or more likely at keypad 108.

Even if encryption is employed on the identification data in the prior art, e.g., prior to transmission from ATM 100 to database 104, the encryption typically occurs within ATM 100 and still requires the entry of non-encrypted identification data from user 106 and the existence of the identification data for some duration of time in ATM 100. Unauthorized access to the identification data may then occur if an unauthorized party is able to gain entry into ATM 100 and intercepts, e.g., via software or hardware implemented in ATM 100, the non-encrypted identification data therein.

Furthermore, if public key cryptography is employed within ATM 100, the storage of the user's private key within ATM 100 renders this private key vulnerable to theft, further exposing the user's account to risk. The stolen password and/or private key may then be employed to allow unauthorized persons to access the user's account to the user's detriment.

In view of the foregoing, there are desired apparatus and methods for conducting transactions with the electronic transaction system while substantially eliminate the risk of unauthorized access to the user's account and unauthorized procurement of the user identification data. Preferably, such an apparatus should be easily portable to permit the user to conveniently and comfortably perform transaction authentication anywhere.

Summary of the Invention

The invention relates, in one embodiment, to a portable transaction arrangement for permitting a user to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system. The charge card terminal is configured to communicate with a charge card for the purpose of conducting the charge card transaction. The charge card is one of a magnetic stripe card and an electronic smart card. The portable transaction arrangement includes an emulation card having an emulation card interface. The emulation card interface emulates an interface of the charge card. The interface of the charge card facilitates communication between the charge card and the charge card terminal. There is also included a portable emulation card configuring device arranged to be used in conjunction with the emulation card, which in turn includes a memory configured to store first charge card data pertaining to a first charge card of the user, and an authentication mechanism. The portable emulation card configuring device is configured to write from the memory the first charge card data to the emulation card if the user is authenticated through the authentication mechanism, thereby allowing the emulation card to appear through the emulation card interface, after writing and for the purpose of conducting the transaction, like the first charge card to the charge card terminal and enabling the charge card terminal to read the first charge card data from the emulation card to conduct the charge card transaction.

In another embodiment, the invention relates to a method for permitting a user to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system. The charge card terminal is configured to interface with a charge card for the purpose of conducting the charge card transaction. The charge card is one of a magnetic stripe card and an electronic smart card. The method includes providing an emulation card having an emulation card interface. The emulation card interface emulates an

interface of the charge card. The interface of the charge card facilitates communication between the charge card and the charge card terminal. There is included providing a portable emulation card configuring device configured to be used in conjunction with the emulation card, which includes a memory configured to store first charge card data pertaining to a first charge card of the user, and an authentication mechanism. The portable emulation card configuring device is configured to write from the memory the first charge card data to the emulation card if the user is authenticated through the authentication mechanism, thereby allowing the emulation card to appear through the emulation card interface, after writing and for the purpose of conducting the transaction, like the first charge card to the charge card terminal and enabling the charge card terminal to read the first charge card data from the emulation card to conduct the charge card transaction.

In yet another embodiment, the invention relates to a method for permitting a user to approve an internet transaction request vis-à-vis a user computer terminal coupled to the internet. The internet transaction request is generated by a first computer coupled to the internet. The method includes sending first digital data from the first computer to the user computer terminal, the first digital data representing the internet transaction request. The method further includes receiving at a second computer coupled to the internet second digital data. The second digital data is manually entered by the user via the user computer terminal. The second digital data represents user-readable encrypted transaction approval data signifying the user's approval of the internet transaction request that is encrypted using a private key of the user by one of a portable electronic authorization device (PEAD) and a portable electronic charge and authorization device (PECAD) from information input by the user into the one of the portable electronic authorization device (PEAD) and the portable electronic charge and authorization device (PECAD). The method additionally includes decrypting, after receiving, the second digital data using a public key of the user.

In yet another embodiment, the invention relates to a computer-implemented method for registering a user of a specific electronic encryption device configured to encrypt data in accordance with a public key encryption scheme. The method includes providing a list of public keys and identification information pertaining to a plurality of electronic encryption devices in a computer database, individual ones of the list of public keys being associated with individual ones of a plurality of electronic encryption devices. The method additionally includes receiving device identification data from the user. The device identification data identifies the specific electronic encryption device. There is also included receiving encrypted user identification data to ascertain an identity of the user. Additionally, there is included associating the device identification data with the specific electronic encryption device in the database, thereby ascertaining a specific public key associated with the specific electronic encryption device from the database. Further, there is included decrypting the encrypted user identification data using the specific public key, and associating the user with the specific electronic encryption device in the database if the decrypting is successful.

These and other advantages of the present invention will become apparent upon reading the following detailed descriptions and studying the various figures of the drawings.

Brief Description of the Drawings

To facilitate discussion, Fig. 1 shows a prior art electronic transaction system, including an automated teller machine (ATM).

Fig. 2 illustrates, in accordance with one embodiment of the present invention, a portable electronic authorization device (PEAD), representing the apparatus for securely approving transactions conducted vis-à-vis an electronic transaction system.

Fig. 3A shows, in one embodiment of the present invention, a simplified schematic of the PEAD of Fig. 2.

Fig. 3B shows, in one embodiment, the format of representative transaction approval data.

Fig. 4 illustrates, in accordance with one embodiment of the present invention, a logic block schematic of the PEAD.

Fig. 5A represents, in accordance with one embodiment of the present invention, a high level hardware implementation of the PEAD.

Fig. 5B illustrates one implementation of a PEAD wherein the PEAD circuitries are implemented on an IC.

Fig. 5C represents an external view of the PEAD of Fig. 5B after being embedded in a card-like package.

Fig. 6A illustrates an external view of the PEAD in accordance with a preferred embodiment of the present invention.

Fig. 6B illustrates, in a simplified manner and in accordance with one aspect of the present invention, the hardware for implementing the PEAD of Fig. 6A

Fig. 7 is a flowchart illustrating, in accordance with one aspect of the present invention, the approval technique employing the inventive PEAD.

Fig. 8 is a flowchart illustrating, in accordance with one aspect of the present invention, steps involved in encrypting transaction approval data using a public key cryptography technique.

Fig. 9 illustrates, in accordance with one aspect of the present invention, a simplified block diagram of a portable electronic charge and authorization device (PECAD).

Fig. 10 is a simplified view of a PECAD, including an emulation card disposed therein, in accordance with one embodiment of the present invention.

Fig. 11 is a simplified flowchart, illustrating in accordance with one embodiment, how a transaction number may be employed in conjunction with a PECAD system to improve transaction security.

Detailed Description of the Preferred Embodiments

Fig. 2 illustrates, in accordance with one embodiment of the present invention, a portable electronic authorization device (PEAD) 200, representing the apparatus for securely approving transactions conducted vis-à-vis an electronic transaction system. With reference to Fig. 2, requesting device 202 may initiate a transaction approval process with PEAD 200 by transmitting to PEAD 200, via communication port 204, a transaction request pertaining to a proposed transaction. Requesting device 202 may represent, for example, an ATM machine, a computer terminal in a network, an automated library check-out terminal, or similar devices for permitting the user to transact business with the electronic transaction system. The proposed transaction may be, for example, a sale transaction of a particular item for a certain amount of money. The transaction request itself may include, for example, the transaction ID, the merchant's name, the merchant's ID, the time of the proposed purchase, and the like. In one embodiment, the transaction request from requesting device 202 may be encrypted for enhanced security but this is not required. Data pertaining to the proposed transaction reaches PEAD 200 via path 206 in Fig. 2.

Port 204 may represent an infrared port to facilitate infrared communication with PEAD 200. Alternatively, port 204 may represent a wireless port for facilitating wireless communication. Port 204 may even represent a contact-type connection port, such as a magnetic read/write mechanism or a plug having electrical contacts for directly plugging PEAD 200 into port 204 to facilitate communication. Other techniques to facilitate communication between requesting device 202 and PEAD 200 are readily appreciable to those skilled.

The data pertaining to proposed transaction(s) may then be reviewed by the user, either on a screen 208 of requesting device 202 or optionally on a

display screen provided with PEAD 200 (not shown in Fig. 2). If the user approves the transaction, e.g., a purchase of an item for a given amount of money, the user may then signify his approval by activating a switch 210 on PEAD 200, which causes an approval message to be created with the user's identification data, encrypted and transmitted back to requesting device 202 via path 212. If the transaction is not approved, the user may simply do nothing and let the transaction request times out after an elapsed time or may activate another switch on PEAD 200 (not shown in Fig. 1), which causes a reject message, either encrypted or non-encrypted, to be transmitted back to the requesting device 202 via path 212.

The present invention is different from the prior art technique of Fig. 1 in that the user is required in the prior art to enter his identification data into the electronic transaction system, e.g., into ATM 100, to authenticate himself. In contrast, the present invention keeps the identification data related to the user secure within PEAD 200 at all times. Transaction approval occurs within PEAD 200, and the data representing such approval is encrypted, again within PEAD 200, prior to being transmitted to the electronic transaction system, e.g., to requesting device 202 in Fig. 2.

Accordingly, even if the approval data is intercepted, its encryption would prevent unauthorized users from employing the identification data for illicit purposes. If public key cryptography is employed to encrypt the approval data, the user's private key is also always kept within PEAD 200. Since the user's private key is required for encryption and is unknown to others, even to the electronic transaction system in one embodiment, the encrypted approval data, if intercepted, would be useless to unauthorized third parties even if the approval data can be deciphered using the user's public key. Again, this is different from prior art authentication techniques wherein encryption takes place within the electronic transaction system and requires the entry of the identification data and/or reading the user's private key from the ID card such as an ATM card, a credit card, and the like. As mentioned earlier, the fact that the prior art electronic transaction system requires this

identification data and/or user's private key exposes these data to risks, e.g., if the requesting device is not secure or open to data interception via software or hardware.

As another difference, the present invention employs the circuitries within the portable electronic authorization device (PEAD) to perform the approval and encryption of the transaction approval data within the PEAD itself. In contrast, prior art data cards are essentially passive devices. For example, prior art ATM cards or credit cards only has a magnetic stripe for storing account information and do not have any facility to perform approval and/or encryption of the transaction approval data. While smart cards or IC cards, which are currently being developed, may contain electronic circuitries, current standards for their implementation still requires a reader associated with the requesting device to read out the identification data and/or user's private key in order for the requesting device to perform any approval and/or encryption. As mentioned earlier, the transmission of these data to the requesting device unnecessarily exposes these data to risks of theft and/or unauthorized interception once transmitted.

It should be borne in mind at this point that although public key cryptography is discussed throughout this disclosure to facilitate ease of understanding and to highlight a particular aspect of the invention, the overall invention is not limited to any particular cryptography algorithm and may be implemented using any conventional cryptography technique, including public key cryptography algorithms such as RSA, Diffie-Hellman, other discrete logarithm systems, elliptic curve systems, or the like. For additional information on some of the different public key cryptography techniques, reference may be made to, for example, the IEEE P1363/D8 Standard Specifications for Public Key Cryptography dated October 5, 1998, available from IEEE Standards Dept. 345 East 7th Street, New York, New York 10017-2349.

As mentioned, transaction approval in the prior art occurs within the electronic transaction system. In contrast, the present invention allows transaction approvals to occur within PEAD 200. The fact that transaction approvals occur entirely within PEAD 200 provides many advantages. By way of example, this feature eliminates the need to have, in one embodiment, the identification data and/or the user's private key in the requesting device. The fact that transaction approvals occur entirely within PEAD 200 (using the user identification data and/or the user's private encryption key that are always kept secure within PEAD 200) substantially enhances the confidentiality of the user identification data and the user's private key, as well as the integrity of the transaction approval process.

Since approval occurs entirely within PEAD 200, the user identification data that is employed to authenticate transactions may be more complicated and elaborate to ensure greater security. By way of example, the user identification data may be more elaborate than a simple password and may include any of the user's name, his birth date, his social security number, or other unique biometrics or unique identifying data such as fingerprint, DNA coding sequence, voice print, or the like. In contrast, prior art authentication techniques limit the user identification data to simple patterns, e.g., simple password of few characters, that are easily memorized by the user since more elaborate identification data may be too difficult to remember or too cumbersome to manually enter. Furthermore, even if the complicated ID data may be stored in the prior art data card, it is still required to be read into the requesting device of the electronic transaction system, again exposing this data to interception or theft once read.

Additional safeguards, which will be described in detail herein, may also be provided to prevent access, whether electronically or by physical means, to the user identification data and/or the user's private key within PEAD 200. Since the identification data and/or the user's private key are never exposed, security risks to the these data are substantially minimized.

Fig. 3A shows, in one embodiment of the present invention, a simplified schematic of PEAD 200 of Fig. 2, including switch 210. Data path 206 is provided for receiving transaction requests from the electronic transaction system, and data path 212 is provided for transmitting transaction approval data back to the electronic transaction system. It should be borne in mind that although two data paths are discussed herein for ease of understanding, these data paths and other data paths herein may, in one embodiment, represent logical data paths and may be implemented via a single physical data connection. Likewise, the different ports herein may represent, in one embodiment, logical data ports for ease of understanding and may in fact be implemented using a single physical port.

When a transaction request, e.g., a withdrawal transaction from an ATM machine in the amount of $200.00, is transmitted via data path 206 to PEAD 200, this transaction is received by encryption logic 300. At this point, the user may review the proposed transaction, e.g., via the display screen provided with the electronic transaction system and/or PEAD 200, and has a choice to either approve or disapprove the proposed transaction. If the user approves the transaction, he may, in one embodiment, activate a switch 210, which causes the transaction approval data to be created and then encrypted by encryption logic 300 prior to being transmitted back to the electronic transaction system via path 212.

Note that the user identification data block 302, which is employed in the transaction approval process, is not directly coupled to paths 206 and 212. In other words, the memory portion storing the user identification data is intentionally decoupled from the input and output ports of PEAD 200 to prevent direct access thereto.

If access to user identification data 302 is desired, e.g., to approve a transaction, the access can only be made by encryption logic block 300. Likewise, it is not possible to directly access the memory portion 304, which stores the user's private key. If access to user's private key 304 is desired,

e.g., to encrypt the transaction approval data, the access can only be made by encryption logic block 300. It should be borne in mind that although user identification 302 and user's private key 304 are shown stored in different memory portions, such illustration is made for ease of understanding and both of these may in fact be stored, in one embodiment, at different addresses on the same memory module.

In some cases, the transaction approval data requires the inclusion of certain pieces of identification data 302. For example, a transaction embodied in the transaction request from the electronic transaction system may be appended with data representative of an "electronic signature" prior to being encrypted and retransmitted back to the electronic transaction system. Fig. 3B shows, in one embodiment, the format of representative transaction approval data 350. With reference to Fig. 3B, transaction data 352, representing a portion of or the entire transaction request received from the electronic transaction system, is appended with certain user identification data 354 and optionally a time stamp 356. The formation of transaction approval data 350 only occurs if the transaction request has already been approved by the user. Once appended, transaction approval data 350 is then encrypted prior to being retransmitted back to the electronic transaction system.

In some cases, it may be desirable to encrypt the transaction request prior to transmission to the PEAD to further enhance security. For example, certain transaction partners, e.g., vendors or other users on the computer network, may wish to keep the information within a transaction request confidential and may prefer to encrypt the transaction request before furnishing it to the PEAD. Data encryption is also desirable when, for example, the user identification data and the user's private key is written into a blank PEAD for the first time to configure a PEAD that is unique to a given user. The configuration data pertaining the user identification data and the user's private key, while must be written only once into PEAD 200 by the issuer of PEAD 200, is preferably encrypted to render them less vulnerable to

theft. Issuers of PEAD 200 may represent, for example, credit card issuers, the government, or any other institution with whom the user maintains an account.

Fig. 4 illustrates, in accordance with one embodiment of the present invention, a schematic of PEAD 200 of Fig. 2. The PEAD 200 of Fig. 4 further employs decryption logic for receiving the encrypted configuration data and optionally the encrypted transaction requests. In Fig. 4, encryption logic 300, user's private key 304, and data paths 206 and 212 are arranged and function substantially as discussed in connection with Fig. 3A.

Transaction requests are normally non-encrypted, i.e., they are received and processed in the manner discussed in connection with Fig. 3A. For highly sensitive transactions, however, the transaction requests may be encrypted and transmitted to PEAD 200 via data path 206 and input into decryption logic 402 to be decrypted. If a public key cryptography is employed, the encrypted transaction requests may be decrypted with a transaction partner public key 404.

Once decrypted, the transaction request is then displayed to the user for approval. The transaction approval data may be furnished to encryption logic 300 via path 406 to be encrypted if approved, e.g., responsive to the activation of switch 210. The encryption is preferably performed with the user's private key 304 if a public key cryptography technique is employed, and the encrypted transaction approval data is then transmitted back to the electronic transaction system via data path 212.

As configuration data typically includes sensitive user identification data and user's private key, it is often encrypted prior to being transmitted to PEAD 200 via data path 408. The encrypted configuration data is received by decryption logic 402 and decrypted therein prior to being written into user identification data block 410 and user's private key block 304. If public key cryptography is employed, the encrypted configuration data may be encrypted by the issuer's private key in the electronic transaction system prior to

transmission and decrypted once received by PEAD 200 with an issuer public key 412.

Note that once the configuration data is decrypted and written into user identification data block 410 and user's private key block 304, the user identification data and user's private key can only be accessed subsequently by encryption logic 300. Also note that there is no direct connection from any of the I/O data paths, e.g., data path 206, 212, or 408, to user identification data block 410 as well to user's private key block 304. Advantageously, the sensitive user identification data and user's private key therein are not susceptible to access from outside once written into respective blocks 410 and 304 (which may, in one implementation, simply represent memory blocks in PEAD 200's memory).

Additionally, the user identification data and the user's private key cannot be updated by those not having the issuer's private key. As represented in Fig. 4, data can only be written into user's private key block 304 and user identification block 410 after it is decrypted via decryption logic 402 with issuer public key 412. Accordingly, unless the updated configuration data has been encrypted using the issuer's private key (which is presumably highly secure), the updated configuration data will not be decrypted and written into respective blocks 304 and 410. Of course if the configuration data within blocks 304 and 410 cannot be updated physically, e.g., they are stored using memory that can be written only once such as PROM (programmable read-only memory), WORM (write once, read many), or the like, the security consideration associated with unauthorized alteration of configuration data is substantially eliminated.

If a greater level of security is desired, the user's private key may be optionally be scrambled or randomized prior to being written into user's private key block 304 by optional scrambler/descrambler logic 413. Scrambler/descrambler logic 413 may, in one embodiment, receive the user's private key, which is furnished by the institution that issues PEAD 200 to the

user, and scrambles and/or randomizes it to generate yet another user's private key and a corresponding user's public key. This scrambled/randomized user's private key is then stored in user's private key block 304, which is now unknown even to the issuer of PEAD 200, and the corresponding user's public key may be made known to the issuer and/or the transaction partners to facilitate transactions. Advantageously, there is no other copy of the scrambled/randomized user's private key anywhere else beside within user's private key block 304.

In an alternative embodiment, there may be employed an optional key generation logic 414 which, responsive to a request from the issuing institution, generates the user's private key and the user's public key on its own, i.e., without first requiring the receipt of a user's private key from the issuing institution and randomizing it. The generated user's private key is then stored in private key block 304 and the public key is made known to the issuing institution and/or the transaction partners to facilitate transactions. In this manner, no version of the user's private key, whether randomized or not, exists outside the PEAD itself. As can be appreciated by those skilled in the art, the use of key generation logic 414 further enhances the confidentiality of the user's private key.

Fig. 5A represents, in accordance with one embodiment of the present invention, a high level hardware implementation of PEAD 200. As shown in Fig. 5A, PEAD 200 includes logic circuitry 502, which may represent a central processing unit such as a microprocessor or a microcontroller, discrete logic, programmable logic, an application-specific integrated circuit (ASIC), or the like, for implementing encryption logic 300 of Fig. 2 and optionally decryption logic 402 of Fig. 4.

Program/data memory 504 stores, among others, the codes which operate PEAD 200 as well as the user identification data and the user's private key. Program/data memory 504 is preferably implemented using some form of non-volatile memory (NVM) such as flash memory, electrically

programmable read-only memory (EPROM), electrically erasable, programmable read-only memory (EEPROM), or the like. Temporary memory 506 serves as a scratch pad for calculation purposes and for temporary storage of data, and may be implemented using some form of random access memory (RAM) such as static RAM or dynamic RAM, which are known in the art. Alternatively, either optical memory, magnetic memory, or other types of memory may be employed to implement program/data memory 504 and/or temporary memory 506.

A bus 508 couples program/data memory 504 and temporary memory 506 with logic circuitry 502. Communication port 510 represents the communication gateway between PEAD 200 and the electronic transaction system and may be implemented using infrared technology, wireless RF technology, a magnetic read/write head, a contact-type plug for facilitating serial or parallel data transmission, or the like. Communication port may also represent, in one embodiment, a PC card port (popularly known to those skilled as a PCMCIA card). Data path 206 inputs transaction requests into logic circuitry 502 while data path 212 outputs transaction approval data from logic circuitry 502 to the electronic transaction system. Optional data path 408, which has been described in Fig. 4, inputs configuration data into PEAD 200 to write the user identification data and the user's private key into program/data memory 504 to uniquely configure PEAD 200 to a particular user.

Again, note that access to program/data memory 504 and the data therein (e.g., the user identification data and the user's private key) can only be made by logic circuitry 502. For example, the user identification data and the user's private key can only be written into program/data memory 504 if this data has been properly encrypted with the issuer's private key. Access to these memory blocks for writing thereto may also be restricted by logic circuitry 502 under appropriate software and/or firmware control.

Similarly, reading the user identification data and accessing the user's private key can only be accomplished via the encryption logic of logic circuitry 502. The advantages to security of this aspect has been discussed in connection with Figs. 3A and 4, the most important point being there is preferably no direct access to the sensitive user identification data and user's private key from the outside. Consequently, the confidentiality and security of these data items are greatly enhanced with the inventive design.

Some type of power source, such as a battery, may be provided as well. If PEAD 200 is implemented as a single-chip design, i.e., substantially all components shown in Fig. 5A are fabricated on a single die, then power is external to the die itself. If contact-type communication is employed, e.g., if PEAD 200 must be plugged into the electronic transaction system to conduct transactions, power external to the entire PEAD may be employed for transaction approvals when plugged in, thereby eliminating the size, weight, and cost penalties associated with having a battery onboard the portable transaction apparatus.

In one embodiment, PEAD 200 may be implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA's) that are currently popular. A PDA such as the Apple Newton®, for example, may be employed to implement PEAD 200.

Fig. 5B illustrates one implementation of a PEAD wherein the circuitries are implemented on an IC. In Fig. 5B, components having like reference numbers to components in Fig. 5A have similar functions. Data paths 408, 206, and 212, which have been described in connection with Fig. 5A, is coupled to a serial I/O circuit 520, which facilitates data transmission and receipt in a serial manner on data path 522 between PEAD 200 and the electronic transaction system. Vcc pin 524 and ground pin 526, which provide power to PEAD 200 of Fig. 5B, are also shown.

Fig. 5C represents an external view of the PEAD of Fig. 5B after being embedded in a card-like package for ease of carrying and insertion into a serial I/O port of the electronic transaction system. Card 550, which embeds the integrated circuit implementing the inventive PEAD, includes, in one embodiment, four external contacts. External serial contacts 552 and 554 carry data and ground respectively to facilitate serial communication with a serial device of an electronic transaction system. External Vcc contact 524 and external ground contact 526, which supply power to the PEAD as discussed in connection with Fig. 5A, are also shown. When card 550 is inserted into an electronic transaction system, it is powered through external contacts 524 and 526, thereby enabling the PEAD circuitries therein to receive transaction requests via external serial contacts 552 and 554, approve the requests within the PEAD if appropriate, encrypt transaction approval data within the PEAD circuitries, and serially communicate the encrypted transaction approval data to the electronic transaction system via external serial contacts 552 and 554.

Fig. 6A represents an external view of a PEAD in accordance with a preferred embodiment of the present invention. PEAD 200 of Fig. 6A is preferably implemented as a small, self-containing package that is sufficiently ruggedized for daily use in the field. Preferably, PEAD 200 of Fig. 6A is small enough to be comfortably carried with the user at all times, e.g., as a key chain attachment or a small package that can easily fit inside a purse or a wallet. The physical enclosure of PEAD 200 is preferably arranged such that the content will be tamper-proof (i.e., if it is opened in an unauthorized manner then the user's private key and/or the user identification data will be destroyed or the PEAD will no longer be able to approve transactions). By way of example, the enclosure may be arranged such that if it is opened, there is a change in the flow of current in a current path, e.g., either the existing current flow is interrupted or a current path that has been idle starts to flow. The change in the flow of current may then force RE

There is shown an infrared communication port 602 for receiving and transmitting data vis-à-vis the electronic transaction system. A small on/off switch 604 permits the user to turn off the PEAD to conserve power when not in use. Approve button 606 permits the user to signify approval of a proposed transaction. Optional skip button 608 permits the user to indicate rejection of a particular transaction. Skip button 608 may be omitted since a transaction request may be understood, in some embodiment, as not being approved if approve button 606 is not activated within a given period of time after receiving the request.

Optional display 610 may be implemented using any type of display technology such as liquid crystal technology. Displays 610 displays, among others, the transaction being proposed for approval. Display 610 may be omitted if desired, in which case the transaction may be viewed, for example, at a display associated with the electronic transaction system itself. Optional user authentication mechanism 612 prevents PEAD 200 from being used for approving transactions unless the user is able to identify himself to PEAD 200 as the rightful and authorized user. Optional user authentication mechanism 612 may require the user to enter a password, to furnish a fingerprint or a voice print, or other biometrics and/or identifying characteristics specific to the authorized user before PEAD 200 can be activated and employed for approving transactions.

Fig. 6B illustrates, in a simplified manner and in accordance with one aspect of the present invention, the hardware for implementing PEAD 200 of Fig. 6A. Battery 652 provides power to the circuitry of PEAD 200. A microcontroller 654 executes codes stored in flash memory 656 and employs random access memory 658 for the execution. In one embodiment, microcontroller 654, flash memory 656, and even random access memory 658 may be implemented on a single chip, e.g., a NC68HC05SCXX family chip from Motorola Inc. of Schaumburg, Illinois such as the NC68HC05SC28. Approve button 606 and optional skip button 608 are coupled to microcontroller 654 to permit the user to indicate approval or rejection of a

particular transaction displayed using display circuitry 660. Communication to and from the electronic transaction system is accomplished under control of microcontroller 654 via an infrared transceiver 662. Power switch 664 permits the user to power off PEAD 200 when not in use to conserve power and to prevent accidental approval.

Fig. 7 is a flowchart illustrating, in accordance with one aspect of the present invention, the approval technique employing the inventive PEAD. In step 702, a transaction request is received at the PEAD from the requesting device associated with the electronic transaction system. In step 704, the user has the option whether to approve or disapprove the transaction proposed. If not approved, e.g., either by activating the skip button of the PEAD or simply allowing the request to time out, nothing will be done.

On the other hand, if the user approves the proposed transaction, the user may activate the approve button to create transaction approval data. The transaction approval data is then encrypted in step 708 within the PEAD. In step 710, the encrypted transaction approval data is transmitted to the requesting device of the electronic transaction system after being encrypted.

Fig. 8 is a flowchart illustrating, in accordance with one aspect of the present invention, the steps involved in encrypting transaction approval data using public key cryptography. In step 802, the transaction approval data package is created. As discussed earlier in connection with Fig. 3B, the transaction approval data may be created by appending any necessary user identification data to a portion of or the entire transaction request. Optionally, a time stamp may also be appended thereto. In step 804, the transaction approval data is encrypted using the user's private key, which is preferably kept secured at all times within the PEAD. Thereafter, the encrypted transaction approval data is transmitted back to the electronic transaction system.

In accordance with one aspect of the present invention, it is recognized that even if the encrypted transaction approval data is intercepted and

decrypted for analysis by a third party, it is not possible to bypass the security features of the invention as long as the user's private key or the user identification data is secure. As mentioned earlier, since the user identification data is not accessible externally, it is always secure within the PEAD. This is unlike the prior art wherein the user is required to enter the identification data, e.g., password, at the electronic transaction system and risks exposure of this sensitive data.

Even if the user identification data is compromised, transaction approval still cannot take place unless there is possession of the user's private key. It would be useless to intercept the encrypted transaction approval data even if one can decrypt it using the user's public key since the transaction partner, e.g., the merchant requesting approval of the transaction, will not accept any transaction approval data not encrypted using the user's private key. Again, since the private key is not accessible externally, it is always secure within the PEAD. This aspect of the invention has great advantages in performing on-line transactions since the user's private key no longer has to be stored in a vulnerable computer file in a workstation, which may be accessible by other parties and may be difficult to conveniently tote along for other authentication tasks.

The fact that the PEAD is implemented in a small, portable package makes it convenient and comfortable for the user to maintain the PEAD within his possession at all times. Even if the PEAD is physically stolen, however, the optional user authentication mechanism, e.g., user authentication mechanism 612 of Fig. 6A, provides an additional level of protection and renders the PEAD useless to all but the properly authenticated user. Of course the user can always notify the issuer of the PEAD if the PEAD is stolen or lost, and the issuer can inform transaction partners to refuse any transaction approval data encrypted with the user's private key of the stolen PEAD.

The fact that the transaction approval data includes the time stamp, the merchant's name, the amount approved, and other relevant data also enhances

the integrity of the transaction approval process. If the merchant inadvertently or intentionally submits multiple transaction approvals to the issuer, the issuer may be able to recognize from these data items that the submissions are duplicates and ignore any duplicate transaction approval data. For example, the issuer may recognize that is it unlikely for a user to purchase multiple identical dinners at the same restaurant at a given time and date.

It is recognized by the inventor herein that although the PEAD and the PEAD-enabled point of sale terminals offer a highly secure system for approving transactions, there exists a well-established and widely available charge card infrastructure, which includes the millions of existing charge card point-of-sale terminals (e.g., charge card readers or ATM terminals) in use worldwide. It is further recognized that even in the absence of the PEAD-enabled point of sale terminals, certain PEAD functionality may offer improved transaction security vis-à-vis the existing charge card infrastructure.

In accordance with another aspect of the present invention, there is provided a portable electronic charge/approval device (PECAD), which not only offers the aforementioned PEAD functionality to permit a user to approve a transaction vis-à-vis a PEAD-enabled point of sale terminal, but also to permit the user to conduct transactions vis-à-vis the existing charge card infrastructures. In particular, the complete PECAD system includes a PECAD and an associated emulation card which conforms to current charge card standards as far as its interface with existing charge card readers is concerned. The emulation card can flexibly be configured by the PECAD to appear as an ordinary charge card to the existing charge card reader. Together, the PECAD and the emulation card form a secure system for conducting transactions vis-à-vis the existing charge card infrastructure.

Note that as the term is employed in the context of this embodiment, charge cards encompass both magnetic-stripe cards and electronic smart cards. The charge cards themselves may represent credit cards (such as Visa or Master Cards), ATM cards, royalty cards, discount cards, as well as any other

type of cards with which a user may employ vis-à-vis a point-of-sale terminal to obtain cash, goods, and/or services.

Prior to conducting a transaction, the PECAD has in its memory charge card data pertaining to one or more charge cards of the user. To perform the PEAD functionality, the memory may also include other data items discussed earlier in connection with the PEAD. The charge card data may be input in advance into the PECAD through an appropriate input port, or may be read in advance from the actual charge cards themselves using an appropriate R/W mechanism of the PECAD.

Since the PECAD contains the PEAD functionality, it may of course be employed to approve transactions vis-à-vis a PEAD-enabled point of sale terminal in the manner earlier discussed in connection with the PEAD. In the absence of a PEAD-enabled point of sale terminal, however, the emulation card is employed instead to conduct the transaction vis-a-vis the existing charge card infrastructure.

To conduct a transaction using the emulation card, the user first requests that the PECAD writes charge card data pertaining to a selected charge card to the emulation card. The selected charge card may be selected by the user prior to writing. Since a single emulation card can emulate any number of charge cards, this single emulation card can advantageously replace the multiple charge cards that a user must carry nowadays. Preferably, the user is first properly authenticated, using an appropriate authentication mechanism associated with the PECAD, prior to being allowed to use the PECAD to write charge card data to the emulation card.

After the emulation card is written with the charge card data associated with a user-selected charge card, the user may employ the emulation card as if it were a charge card for the purpose of completing the transaction. That is, since the emulation card conforms to the I/O requirements of existing charge cards and charge card readers, it may be read by an existing charge card reader as if it were a charge card.

Once the transaction is completed, the user may optionally employ the PECAD to erase the charge card data from the emulation card, thereby rendering the emulation card useless for the purpose of conducting further transactions until the properly authenticated user again authorizes the PECAD to write charge card data into the emulation card. If the emulation card emulates an electronic smart card, the emulation card may be rendered incapable of use for other transactions by, for example, configuring the registers or flags within the emulation card appropriately. Thus, even if the emulation card is stolen, it is useless to an unauthorized user . Furthermore, even if the emulation card and the PECAD are stolen together, the emulation card itself cannot be written with charge card data unless the user is properly authenticated. This is in sharp contrast to the existing situation wherein, for example, a stolen credit card still contains in its magnetic stripe all the necessary information to conduct a transaction. For further security, the emulation card itself may be physically signed by the properly authorized user and may contain a picture of the authorized user to allow merchants to visually ascertain whether the person conducting the transaction is in fact the rightful owner of the emulation card.

In a preferred embodiment, each emulation card is matched, in a substantially unique manner, with a specific PECAD to further enhance security. In this situation, a given PECAD can only write charge card data into the emulation card uniquely associated with it. By way of example, an emulation card may be endowed with appropriate optically encrypted marks (such as holograms), magnetically encrypted marks (such as magnetically stored bits) or mechanically encrypted marks (such as randomly spaced holes) so that it can be written only by a specific PECAD.

Preferably, each emulation card is matched with a single unique PECAD. It should be noted, however, this unique matching aspect is not required to be a mathematical absolute (although such may be preferred). One skilled in the art will readily appreciate that given a sufficiently large number of issued emulation cards and PECAD, some overlap may occur that renders it

possible (albeit remotely in real life) that a given emulation card may be recognized by more than one PECAD. In fact, the issuer or manufacturer may possess a master PECAD that is capable of recognizing a number of issued emulation cards. Thus, the association between an emulation card and a PECAD is substantially unique in the sense that a door key is substantially unique to each door lock, not ruling out the potentiality that a manufacturer may choose to make an emulation card absolutely unique relative to a given PECAD or the remote possibility that in the millions of door locks manufactured, a given key may open more than one door lock. Preferably, the encrypted marks and geographic distribution pattern of the emulation cards/PECADs (e.g., within the same city or state) be arranged such that such remote possibility is minimized.

Because each emulation is substantially uniquely matched with a specific PECAD, even if a PECAD is stolen and the authentication mechanism is successfully bypassed by a person intending to commit fraud, the stolen PECAD still cannot be used to write charge card data into any arbitrary blank emulation card for the purpose of conducting fraudulent transactions. As a further advantage, the requirement that a given PECAD can only write (after proper authentication) to the emulation card substantially uniquely associated with it substantially eliminates the accidental overwriting of an existing charge card by the PECAD.

Fig. 9 illustrates, in accordance with one aspect of the present invention, a simplified block diagram of a PECAD 902. In Fig. 9, a memory 904 is preferably nonvolatile, tamper-proof memory and serves the same function as the memory circuit in the PEAD, except that memory 904 may also be employed to store the encrypted charge card data pertaining to one or more charge cards of the user. Encryption logic 906 performs the same encryption/decryption/security function as the encryption logic discussed in connection with the PEAD. That is, access to data stored in memory 904, including the user's private key, the user's personal data, and the charge card data, is preferably facilitated only through encryption logic 906.

Authentication mechanism 908 performs the same user authentication function discussed in connection with the PEAD. I/O circuitry 910 represents the circuitry that permits the PECAD to communicate with a PEAD-enabled point of sale terminal if it is available for the purpose of approving transactions. The transaction approval aspect has been discussed earlier in connection with the PEAD and will not be belabored here. I/O circuitry 910 may be omitted on certain PECAD models if it is expected that such PECAD models do not communicate with a PEAD point of sale terminal and are employed only to configure emulation cards for the purpose of conducting transactions vis-à-vis the existing charge card infrastructure.

Card R/W mechanism 912 represents the mechanism employed to write to selected charge card data to the emulation card and to erase the emulation card after the transaction is completed. If the charge card data is acquired by reading in existing charge cards, card R/W mechanism 912 also includes the ability to read in existing charge cards for the purpose of storing the charge card data to memory 904 (through encryption logic 906). Note that data read through card R/W mechanism 912 is encrypted by encryption logic 906 prior to being stored within memory 904. Likewise, stored data (such as charge card data) in memory 904 is first decrypted by encryption logic 906 prior to being written to an emulation card via card R/W mechanism 912.

Fig. 10 is a simplified sketch of a PECAD 1002, including an emulation card 1004 disposed therein. Emulation card 1004 is removable from slot 1006 for the purpose of completing transactions vis-a-vis an existing charge card reader. In the example of Fig. 10, emulation card 1004 includes a magnetic stripe 1008 to emulate a magnetic stripe charge card. As mentioned earlier, however, emulation card 1004 may be configured to emulate any type of charge card interface, including IC contacts. A card R/W mechanism 1010 is shown in an outline format to indicate that it is part of PECAD 1002. Through card R/W mechanism 1010, data may be read from an existing charge card or written to an emulation card. Key pads 1015 can be used as authentication mechanism as described as in 612 as well as 908. User can key

in the password or PIN to activate the PECAD to write the charge card data to the emulation card 1004.

Approve button 1012 is substantially similar to approve button 606 of Fig. 6A and may be employed to approve a transaction via a PEAD-enabled point of sale terminal. Card button 1014 on the other hand indicates the user's desire to complete the transaction via the emulation card. Card selector buttons 1016(a)-(d) are exemplary selections which may be chosen by the user to select the specific charge card that may be employed to conduct the transaction. A display 1018 may be employed to display the charge card data, such as charge card number, expiration date, name of holder, etc. of the selected charge card to allow a merchant to copy such information, if desired, to complete the transaction.

In accordance with another aspect of the present invention, transaction security is further enhanced by using the PECAD to write an encrypted transaction number or other encrypted data that has been encrypted using the user's private key (which is stored in secure nonvolatile memory of the PECAD) to the emulation card. Fig. 11 illustrates, in accordance with one embodiment, this aspect of the present invention. In step 1102, a unique transaction number is generated and encrypted with the user's private key for each transaction. In step 1104, the encrypted transaction number is written from the PECAD to the emulation card. If the emulation card emulates a magnetic stripe card, for example, the encrypted transaction number may be written to one of the existing but unused tracks or one of the reserve tracks, e.g., track 3 on the magnetic stripe. In step 1106, software in the charge card reader may instruct the charge card reader to receive the encrypted transaction number, which is then authenticated using a user's public key that has been obtained from a credentialed third party (step 1108); or in step 1106 , the charge card reader reads in the encrypted transaction number, which is then sent to the credit clearance center such as Master Card or Visa Card and the credit clearance center would authenticate the user by using a user's public key that has been obtained from a credentialed third party (step 1108). Typically, some form of user identification may be sent to the credentialed third party to facilitate obtaining the public key. By way of example, the user ID or the public

key ID may be read by the charge card reader and transmitted to the credentialed third party to obtain the public key. The public key ID may represent, for example, the unique pattern of bits in the public key (e.g., the lowest 32 bits or 64 bits) that may be transmitted to the receiving site for public key searching and decryption. If authenticated, the transaction is then approved, enabling the merchant to release the goods/service to the user (step 1110).

As can be appreciated from the foregoing, the invention requires substantially no hardware change to the existing charge card readers and the existing charge card infrastructure. The change merely relates to software change, which instructs the existing charge card reader to read in the encrypted transaction number and which authenticates the encrypted transaction number using a user's public key obtained from a credentialed third party.

Further, there may be no change at all in the charge card reader. Instead, the credit clearance center software may be modified to authenticate the encrypted transaction number using a user's public key obtained from a credentialed third party. The charge card reader just read in all the data from the charge card or emulation card and verbatimly send all the information to the credit clearance center for approval. In this manner, this embodiment minimizes the changes that need to be made to the existing charge card infrastructure (i.e., changes only have to be made at a single location in the credit clearance center, and not in the millions of charge card readers in existence).

If additional security is desired, the user may key in at the PECAD the transaction amount and/or the time of transaction. These pieces of data may also be encrypted using the user's private key and written to the emulation card to be received by the charge card reader and decrypted at the credit clearance center using the user's public key, which is again preferably obtained from a credentialed third party. In this case, approval of the transaction is given only if the transaction is for the amount indicated in the encrypted and received transaction amount and/or if the transaction occurs within a predefined time period of the encrypted and received transaction time (which was written from the PECAD to the emulation card previously). Thus, even if

the emulation card is stolen, it is useless for other subsequent transactions, even if erasure or reconfiguration of the emulation card did not occur.

In the internet transaction, a user can approve the transaction using PEAD or PECAD by encrypting the amount he approved using his own private key stored in the PEAD and PECAD. Thereafter, he can copy the encrypted information displayed on the PEAD display 610 or PECAD display 1002 to the Internet by keying in the information through the keyboard. The encrypted information displayed on the PEAD display 610 or PECAD display 1002 is preferably in a human readable format such as in alpha numeric string to render it simple for the user to read and manually enter (by for example keying in or by speech command) to the computer connected through the Internet to conduct the Internet transaction. If necessary, one can also encrypt the credit card number together with the transaction information using PEAD or PECAD to conduct secure Internet transactions. Of course the manual entering/keying technique, while desirable for backward compatibility, may be equally substituted by other forms of data entry, e.g., wireless or infrared communication via an appropriate port in the computer and PECAD (or PEAD) to allow data to be transmitted over the Internet.

As mentioned earlier, it is preferable that authentication of the user's identity be ascertained using the user's public key that is kept by a credentialed third party. The credentialed third party may represent, for example, any entity in which the public has a fairly high level of trust, such as an organization known to have or has a self-interest to have a trustworthy reputation. Examples include government organizations, banks, large corporations, or the like.

The credentialed party maintains a PECAD public key directory service that associates the list of manufacturer-provided public keys with users. When the user first acquires (via purchase or issuance by an issuer, for example) a PECAD, the user can register his ownership of the PECAD with the credentialed third party. Depending on the integrity of the registration process, the user is assigned a validation level, which indicates the degree of confidence that the person completing the registration is in fact who he says he is.

By way of example, the user may register simply by furnishing via email, phone, or regular mail personal information such as social security number, home address and home phone number, along with the PECAD serial number and public key signature (which is a unique sequence of numbers assigned by the manufacturer to a particular PECAD and which can be read from the PECAD by pressing a designated sequence of keys). The PECAD public key directory center may then use the PECAD serial number provided by the user as the unique searching ID to search for the Public Key in the database, once it finds the Public Key and it will use the Public Key signature provided by the user to verify against the Public Key in the database. If the verification is successful, then the user may be registered. Otherwise the user will be rejected. The public key is preferably unique.

The more secure way to register a user's ownership may be as follows (the process usually occurs at the place of purchase of the PECAD/PEAD or at the issuer, e.g., a bank). The issuer first activates the PEAD/PECAD using the manufacturer-provided password. Thereafter, the PEAD/PECAD user may overwrite the manufacturer-provided password with the user's password or other authentication mechanism(s). The user may then instruct the PEAD/PECAD to internally generate a new pair of private/public key (called user private key and user public key) inside the PEAD/PECAD. The user may also instruct the PEAD/PECAD to encrypt the personal information (such as social security information, home address, etc.) and the new user public key using the manufacturer-provided private key, which is pre-stored in the PEAD/PECAD to generate the user registration message. This manufacturer-provided private/public key pair may be generated by the PEAD/PECAD when the PEAD/PECAD is manufactured.

The issuer may then encrypt the PEAD/PECAD serial number and user registration message using the public key directory service center's public key to generate the registration message and transmit the registration message to the public key directory service center. Upon receiving the registration message, the public key directory service center may then decrypt the registration message using its own private key. Thereafter, the public key directory service center may use the PEAD/PECAD serial number to search for the manufacturer-provided public key

found in the database. If the decryption is successful, then update the manufacturer-provided public key with the new user public key in the directory service database and update the personal information in the directory service database and generate the public key ID either using, for example, the person name + phone number or the lowest 32-bit (or 64 bit) of the public key for future referencing purposes. On the other hand, if decryption is unsuccessful, the user may then be rejected.

This registration process is generally accorded a low validation level since it is possible that someone other than the user may have fraudulently obtained the user's personal information for the purpose of registering ownership (and making the user responsible for the fraudulent charges that follow once registration is completed and the PECAD is activated).

An intermediate validation level may be obtained by furnishing, in addition to the information provided to acquire a low validation level, information which offers a higher degree of confidence that the person furnishing the information is indeed who he says he is. By way of example, the addition information may take the form of a photograph, signature, notary public's seal, or a combination of the above. A high validation level may be obtained by furnishing information with offers an even higher degree of confidence that the person furnishing the information is indeed who he says he is. By way of example, the registrant may appear in person at the PECAD public key directory center to present a photograph, a signature, a biometrics sample (such as fingerprint, retina scan, DNA print, or the like) or a combination of the above.

Once registration is completed, the PECAD public key directory by the credentialed third party may be consulted by credit clearance centers or merchants for the purpose of authenticating the user and approving transactions.

The PECAD public key directory may also be enhanced by establishing an insurance policy that protects merchants or credit clearance centers from financial loss due to, for example, fraud stemming from a defective registration process. The coverage provided by the insurance policy may be scaled according to the validation level, with the higher validation levels being eligible for a higher amount of coverage.

While this invention has been described in terms of several preferred embodiments, there are alterations, permutations, and equivalents which fall within the scope of this invention. It should also be noted that there are many alternative ways of implementing the methods and apparatuses of the present invention. By way of example, while the discussion herein has focused on transaction approvals, it should be apparent to those skilled that the PEAD may be employed to conduct any kind of transaction vis-à-vis an electronic transaction system any time secured data transmission from the user to the electronic transaction system is preferred. For example, the PEAD may be employed for logging into highly sensitive computer systems or facilities. When so implemented, the computer terminal with which the PEAD communicates may be equipped with an infrared port, a magnetic reader port, or a contact-type plug for communication with the PEAD. The user may then employ the PEAD to perform any type of authentication tasks online.

As a further example, the PEAD may be employed to "sign" any computer file for authentication purposes (e.g., to authenticate the date or the user). The transaction approval data may then be saved along with the file to be authenticated for future reference. Note that the transaction authentication data is again tamper-proof since any transaction authentication data not encrypted using the user's private key will not be accepted as authentic. Also, it should be apparent that if the PEAD is employed to approve only predefined transactions, the transaction data may be stored in advance within the PEAD and do not need to be received from externally by the PEAD. It is therefore intended that the following appended claims be interpreted as including all such alterations, permutations, and equivalents as fall within the true spirit and scope of the present invention.

What is claimed is

1. A portable transaction arrangement for permitting a user to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system, said charge card terminal being configured to communicate with a charge card for the purpose of conducting said charge card transaction, said charge card being one of a magnetic stripe card and an electronic smart card, comprising:

an emulation card having an emulation card interface, said emulation card interface emulates an interface of said charge card, said interface of said charge card facilitating communication between said charge card and said charge card terminal;

a portable emulation card configuring device arranged to be used in conjunction with said emulation card, including

a memory configured to store first charge card data pertaining to a first charge card of said user, and

an authentication mechanism, said portable emulation card configuring device being configured to write from said memory said first charge card data to said emulation card if said user is authenticated through said authentication mechanism, thereby allowing said emulation card to appear through said emulation card interface, after writing and for the purpose of conducting said transaction, like said first charge card to said charge card terminal and enabling said charge card terminal to read said first charge card data from said emulation card to conduct said charge card transaction.

2. The portable transaction arrangement of claim 1 wherein said emulation card includes a unique identification mark for the purpose of substantially uniquely associating said emulation card with said portable emulation card configuring device.

3. The portable transaction arrangement of claim 1 wherein said charge card is a magnetic stripe automated teller machine (ATM) card, said charge card terminal being an automated teller machine (ATM) terminal.

4. The portable transaction arrangement of claim 1 wherein said charge card is a magnetic stripe card, said charge card terminal being one of an automated teller machine (ATM) terminal and a point of sale terminal.

5. The portable transaction arrangement of claim 1 wherein said charge card is an electronic smart card.

6. The portable transaction arrangement of claim 1 wherein said portable emulation card configuring device is configured to erase said first charge card data from said emulation card upon completion of said charge card transaction.

7. The portable transaction arrangement of claim 1 wherein said portable emulation card configuring device further comprises encryption logic disposed between said emulation card interface and said memory, said encryption logic providing secured access between said emulation card interface and said memory.

8. The portable transaction arrangement of claim 7 wherein said emulation card configuring device includes a charge card selection mechanism, said charge card selection mechanism enabling said user to chose said first charge card of said user among said plurality of charge cards whose charge card data is also stored in said memory.

9. The portable transaction arrangement of claim 8 wherein said memory stores only charge card data for a single person.

10. The portable transaction arrangement of claim 1 wherein said authentication mechanism includes an input mechanism for accepting a password comprising an alphanumeric string from said user for the purpose of authentication.

11. The portable transaction arrangement of claim 1 wherein said authentication mechanism employs biometrics for authentication.

12 The portable transaction arrangement of claim 1 wherein said authentication mechanism employs fingerprint for authentication.

13. The portable transaction arrangement of claim 7 wherein said portable emulation card configuring device is further configured to write an encrypted transaction number to said emulation card, said encrypted transaction number being encrypted by said private key.

14. The portable transaction arrangement of claim 7 wherein said memory is configured to store a private key for encrypting data in accordance with a public key/private key encryption scheme, said private key being inaccessible from outside said portable emulation card configuring device except through said encryption logic.

15. The portable transaction arrangement of claim 14 wherein said portable emulation card configuring device is further configured to write encrypted transaction information to said emulation card, said encrypted transaction information being encrypted by said private key and includes at least one of a transaction time and a transaction amount pertaining to said charge card transaction, said encrypted transaction information being readable by said charge card terminal and renders said emulation card valid only for said charge card transaction.

16. The portable transaction arrangement of claim 15 wherein said encrypted transaction information includes said transaction time, said emulation card is invalid for the purpose of completing a given charge card transaction if said given charge card transaction is not completed within a predefined time period of said transaction time.

17. A method for permitting a user to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system, said charge card terminal being configured to interface with a charge card for the purpose of conducting said charge card transaction, said charge card being one of a magnetic stripe card and an electronic smart card, comprising:

providing an emulation card having an emulation card interface, said emulation card interface emulates an interface of said charge card, said interface of

said charge card facilitating communication between said charge card and said charge card terminal;

providing a portable emulation card configuring device configured to be used in conjunction with said emulation card, including

a memory configured to store first charge card data pertaining to a first charge card of said user, and

an authentication mechanism, said portable emulation card configuring device being configured to write from said memory said first charge card data to said emulation card if said user is authenticated through said authentication mechanism, thereby allowing said emulation card to appear through said emulation card interface, after writing and for the purpose of conducting said transaction, like said first charge card to said charge card terminal and enabling said charge card terminal to read said first charge card data from said emulation card to conduct said charge card transaction.

18. The method of claim 17 wherein said charge card is a magnetic stripe automated teller machine (ATM) card, said charge card terminal being an automated teller machine (ATM) terminal.

19. The method of claim 17 wherein said charge card is a magnetic stripe card, said charge card terminal being one of an automated teller machine (ATM) terminal and a point of sale terminal.

20. The method of claim 17 wherein said charge card is an electronic smart card.

21. The method of claim 17 wherein said portable emulation card configuring device is configured to erase said first charge card data from said emulation card upon completion of said charge card transaction.

22. The method of claim 17 wherein said portable emulation card configuring device further comprising encryption logic disposed between said emulation card interface and said memory, said encryption logic providing secured access between said emulation card interface and said memory.

23. The method of claim 22 wherein said memory is configured to store a private key for encrypting data in accordance with a public key/private key encryption scheme, said private key being inaccessible from outside said portable emulation card configuring device except through said encryption logic.

24. The method of claim 17 whereby said portable emulation card configuring device is configured to be incapable of writing charge card data to another card, said another card representing one of an emulation card not substantially uniquely associated with said portable emulation card configuring device and a charge card.

25. The method of claim 17 wherein said emulation card includes a unique identification mark for the purpose of substantially uniquely associating said emulation card with said portable emulation card configuring device.

26. The method of claim 23 wherein said emulation card configuring device includes a charge card selection mechanism, said charge card selection mechanism enabling said user to chose said first charge card of said user among a plurality of charge cards whose charge card data is also stored in said memory.

27. The method of claim 26 wherein said memory stores only charge card data for a single person.

28. The method of claim 17 wherein said authentication mechanism includes an input mechanism for accepting a password comprising an alphanumeric string from said user for the purpose of authentication.

29. The portable transaction arrangement of claim 17 wherein said authentication mechanism employs biometrics for authentication.

30 The method of claim 17 wherein said authentication mechanism employs fingerprint for authentication.

31. The method of claim 23 wherein said portable emulation card configuring device is further configured to write an encrypted transaction number to said emulation card, said encrypted transaction number being encrypted by said private key.

32. The method of claim 23 wherein said portable emulation card configuring device is further configured to write encrypted transaction information to said emulation card, said encrypted transaction information being encrypted by said private key and includes at least one of a transaction time and a transaction amount pertaining to said charge card transaction, said encrypted transaction information being readable by said charge card terminal and renders said emulation card valid only for said charge card transaction.

33. The method of claim 23 wherein said encrypted transaction information includes said transaction time, said emulation card is invalid for the purpose of completing a given charge card transaction if said given charge card transaction is not completed within a predefined time period of said transaction time.

34. The method of claim 23 further comprising obtaining a public key from a credentialed third party to decrypt data read from said emulation card, said data being encrypted by said portable emulation card configuration device using said private key.

35. A portable transaction arrangement for permitting a user to use an emulation card to conduct a charge card transaction vis-à-vis a charge card terminal of an electronic transaction system, comprising:

portable emulation card configuring means configured to be used in conjunction with said emulation card, and having a function of writing to said emulation card, including

memory means configured to store authentication data and first charge card data pertaining to a first charge card of said user, said emulation card having an emulation card interface that emulates an interface of said first charge card, said charge card terminal being configured to communicate with said first charge card through said interface of said first charge card, said charge card being one of a magnetic stripe card and an electronic smart card, and

authentication means arranged to authenticate said user using said authentication data stored in said memory means, said portable emulation card configuring means being configured to write from said memory means said first

charge card data pertaining to said first charge card to said emulation card if said user is authenticated through said authentication means, thereby allowing said emulation card to appear through said emulation card interface, after writing and for the purpose of conducting said transaction, like said first charge card to said charge card terminal and enabling said charge card terminal to read said first charge card data from said emulation card to conduct said transaction.

36. The portable transaction arrangement of claim 35 further comprising encryption logic disposed between said emulation card interface and said memory means, said encryption logic providing secured access between said emulation card interface and said memory means.

37. The portable transaction arrangement of claim 35 wherein said charge card is a magnetic stripe automated teller machine (ATM) card, said charge card terminal being an automated teller machine (ATM) terminal.

38. The portable transaction arrangement of claim 35 wherein said charge card is a magnetic stripe card, said charge card terminal being one of an automated teller machine (ATM) terminal and a point of sale terminal.

39. The portable transaction arrangement of claim 35 wherein said charge card is an electronic smart card.

40. The portable transaction arrangement of claim 35 wherein said portable emulation card configuring means is configured to erase said first charge card data from said emulation card upon completion of said charge card transaction.

41. The portable transaction arrangement of claim 35 wherein said portable emulation card configuring means further comprising encryption logic coupled to said memory means, said encryption logic being disposed to provide secured access to said memory means.

42. The portable transaction arrangement of claim 41 wherein said memory means is configured to store a private key for encrypting data in accordance with a public

key/private key encryption scheme, said private key being inaccessible from outside said portable emulation card configuring means except through said encryption logic.

43. The portable transaction arrangement of claim 42 whereby said portable emulation card configuring means is configured to be incapable of writing charge card data to another emulation card, said another emulation card representing an emulation card not substantially uniquely associated with said portable emulation card configuring means.

44. The portable transaction arrangement of claim 43 wherein said emulation card includes a unique identification mark for the purpose of substantially uniquely associating said emulation card with said portable emulation card configuring means.

45. The portable transaction arrangement of claim 35 wherein said emulation card configuring means includes a charge card selection mechanism, said charge card selection mechanism enabling said user to chose said first charge card among a plurality of charge cards whose charge card data is also stored in said memory means.

46. The portable transaction arrangement of claim 45 wherein said memory means stores only charge card data for a single person.

47. The portable transaction arrangement of claim 35 wherein said authentication means includes an input mechanism for accepting a password comprising an alphanumeric string from said user for the purpose of authentication.

48. The portable transaction arrangement of claim 42 wherein said portable emulation card configuring means is further configured to write an encrypted transaction number to said emulation card, said encrypted transaction number being readable by said charge card terminal, said encrypted transaction number being encrypted by said private key.

49. The portable transaction arrangement of claim 42 wherein said portable emulation card configuring means is further configured to write encrypted transaction information to said emulation card, said encrypted transaction information being encrypted by said private key and includes at least one of a transaction time and a

transaction amount pertaining to said charge card transaction, said encrypted transaction information being readable by said charge card terminal and renders said emulation card valid only for said charge card transaction.

50. The portable transaction arrangement of claim 42 wherein said encrypted transaction information includes said transaction time, said emulation card is invalid for the purpose of completing a given charge card transaction if said given charge card transaction is not completed within a predefined time period of said transaction time.

51. A portable transaction arrangement for permitting a user to conduct a transaction vis-à-vis an electronic transaction system, comprising:

a charge card terminal interfacing subsystem, including

an emulation card having an emulation card interface, said emulation card interface emulating an interface of a charge card, said charge card being one of a magnetic stripe card and an electronic smart card, said interface of said charge card facilitating communication between said charge card and a charge card terminal of said electronic transaction system; and

a portable emulation card configuring device arranged to be used in conjunction with said emulation card, including

a first memory portion configured to store charge card data pertaining to a charge card of said user, and

an authentication mechanism, said portable emulation card configuring device being configured to write from said memory said charge card data pertaining to said charge card of said user to said emulation card if said user is authenticated through said authentication mechanism, thereby allowing said emulation card to appear through said emulation card interface, after writing and for the purpose of conducting said transaction, like said charge card of said user to said charge card terminal and enabling said charge card terminal to read said charge card data from said emulation card to conduct said transaction; and

an electronic authorization interfacing subsystem, including

first logic circuit configured to receive first digital data representative of a transaction request pertaining to said transaction from said electronic transaction system,

second logic circuit configured to form second digital data responsive to said transaction request received by said first logic circuit if said transaction request is approved by said user, said second digital data representing encrypted data signifying an approval by said user of said transaction request; and

transmission circuitry coupled to said second logic circuit, said transmission circuitry being configured to transmit said second digital data from said portable transaction arrangement to said electronic transaction system if said user approves said transaction request.

52. The portable transaction arrangement of claim 51 wherein said portable emulation card configuring device further comprises encryption logic disposed between said emulation card interface and said first memory portion, said encryption logic providing secured access between said emulation card interface and said first memory portion.

53. The portable transaction arrangement of claim 51 wherein said emulation card includes a unique identification mark for the purpose of substantially uniquely associating said emulation card with said portable emulation card configuring device.

54. The portable transaction arrangement of claim 51 wherein said portable emulation card configuring device further comprising encryption logic coupled to said first memory portion, said encryption logic being disposed to provide secured access to said first memory portion.

55. The portable transaction arrangement of claim 54 wherein said portable emulation card configuring device further comprises a second memory portion coupled to said encrypted logic, said second memory portion being configured to store a private key for encrypting data in accordance with a public key/private key encryption scheme, said encryption logic also being disposed to provide secured access to said second memory portion.

56. The portable transaction arrangement of claim 55 wherein said emulation card configuring device includes a charge card selection mechanism, said charge card selection mechanism enabling said user to chose said charge card of said user among a plurality of charge cards whose charge card data is also stored in said first memory portion.

57. The portable transaction arrangement of claim 55 wherein said authentication mechanism includes an input mechanism for accepting a password comprising an alphanumeric string from said user for the purpose of authentication.

58. The portable transaction arrangement of claim 55 wherein said authentication mechanism employs biometrics for authentication.

59. The portable transaction arrangement of claim 55 wherein said portable emulation card configuring device is further configured to write an encrypted transaction number to said emulation card, said encrypted transaction number being encrypted by said private key.

60. The portable transaction arrangement of claim 55 wherein said portable emulation card configuring device is further configured to write encrypted transaction information to said emulation card, said encrypted transaction information being encrypted by said private key and includes at least one of a transaction time and a transaction amount pertaining to said charge card transaction, said encrypted transaction information being readable by said charge card terminal and renders said emulation card valid only for said charge card transaction.

61. The portable transaction arrangement of claim 60 wherein said encrypted transaction information includes said transaction time, said emulation card is invalid for the purpose of completing a given charge card transaction if said given charge card transaction is not completed within a predefined time period of said transaction time.

62. The portable transaction arrangement of claim 51 wherein said charge card is a magnetic stripe automated teller machine (ATM) card, said charge card terminal being an automated teller machine (ATM) terminal.

63. The portable transaction arrangement of claim 51 wherein said charge card is a magnetic stripe card, said charge card terminal being a point of sale terminal.

64. The portable transaction arrangement of claim 51 wherein said charge card is an electronic smart card.

65. The portable transaction arrangement of claim 51 wherein said portable emulation card configuring device is configured to erase said first charge card data from said emulation card upon completion of said charge card transaction.

66. A method for permitting a user to approve an internet transaction request vis-à-vis a user computer terminal coupled to the internet, said internet transaction request being generated by a first computer coupled to said internet, comprising:

sending first digital data from said first computer to said user computer terminal, said first digital data representing said internet transaction request;

receiving at a second computer coupled to said internet second digital data, said second digital data being manually entered by said user via said user computer terminal, said second digital data representing user-readable encrypted transaction approval data signifying said user's approval of said internet transaction request, said second digital data being encrypted using a private key of said user by one of a portable electronic authorization device (PEAD) and a portable electronic charge and authorization device (PECAD) from information input by said user into said one of said portable electronic authorization device (PEAD) and said portable electronic charge and authorization device (PECAD); and

decrypting, after said receiving, said second digital data using a public key of said user.

67. The method of claim 66 further comprising receiving said public key from a credentialed third party.

68. The method of claim 66 wherein said information input by said user into said one of said portable electronic authorization device (PEAD) and said portable

electronic charge and authorization device (PECAD) includes a transaction amount associated said internet transaction request.

69. The method of claim 66 wherein said information input by said user into said one of said portable electronic authorization device (PEAD) and said portable electronic charge and authorization device (PECAD) also includes a credit card number to be charged.

70. The method of claim 66 wherein said second digital data is encrypted using said portable electronic authorization device (PEAD).

71. The method of claim 66 wherein said second digital data is encrypted using said portable electronic charge and authorization device (PECAD).

72. The method of claim 66 wherein said first computer and said second computer is the same computer.

73. The method of claim 66 wherein said first computer and said second computer are different computers.

74. A computer-implemented method for registering a user of a specific electronic encryption device configured to encrypt data in accordance with a public key encryption scheme, comprising:

providing a list of public keys and identification information pertaining to a plurality of electronic encryption devices in a computer database, individual ones of said list of public keys being associated with individual ones of a plurality of electronic encryption devices;

receiving device identification data from said user, said device identification data identifying said specific electronic encryption device;

receiving encrypted user identification data to ascertain an identity of said user;

associating said device identification data with said specific electronic encryption device in said database, thereby ascertaining a specific public key associated with said specific electronic encryption device from said database;

decrypting said encrypted user identification data using said specific public key; and

associating said user with said specific electronic encryption device in said database if said decrypting is successful.

75. The method of claim 74 wherein said specific electronic encryption device represents a portable electronic authorization device.

76. The method of claim 74 wherein said specific electronic encryption device represents a portable electronic charge and authorization device.

77. The method of claim 74 further including assigning a validation level to said user in said database, said validation level being assigned in accordance to a level of confidence associated with said user identification data.

78. The method of claim 77 wherein said validation level represents one of a high level and a low level, said high level being assigned to said user in said database if said user presents said user identification data in person to permit verification of said user identity against said user identification data.

79. The method of claim 78 wherein said low level is assigned to said user in said database if said user does not present said user identification data in person to permit said verification of said user identity against said user identification data.

80. The method of claim 77 wherein said validation level scales with an insurance coverage amount provided by an insurance policy configured to protect against fraudulent registration of said specific electronic encryption device.

81. A computer-implemented arrangement for registering a user of a specific electronic encryption device configured to encrypt data in accordance with a public key encryption scheme, comprising:

means for storing a list of public keys and identification information pertaining to a plurality of electronic encryption devices, individual public keys in said list of public keys being associated with individual ones of said plurality of electronic encryption devices;

means for ascertaining, from encrypted user-supplied device identification data, said identification information, and said list of public keys, a specific public key associated with said specific electronic encryption device, whereby said encrypted user-supplied device identification data identifies said specific electronic encryption device;

means for decrypting said encrypted user-supplied identification data received from said user using said specific public key; and

means for associating said user with said specific electronic encryption device if said decrypting is successful.

82. The computer-implemented arrangement of claim 81 wherein said specific electronic encryption device represents a portable electronic authorization device.

83. The computer-implemented arrangement of claim 81 wherein said specific electronic encryption device represents a portable electronic charge and authorization device.

84. The computer-implemented arrangement of claim 81 further including means for assigning a validation level to said user in said database, said validation level being assigned in accordance to a level of confidence associated with an identity of said user.

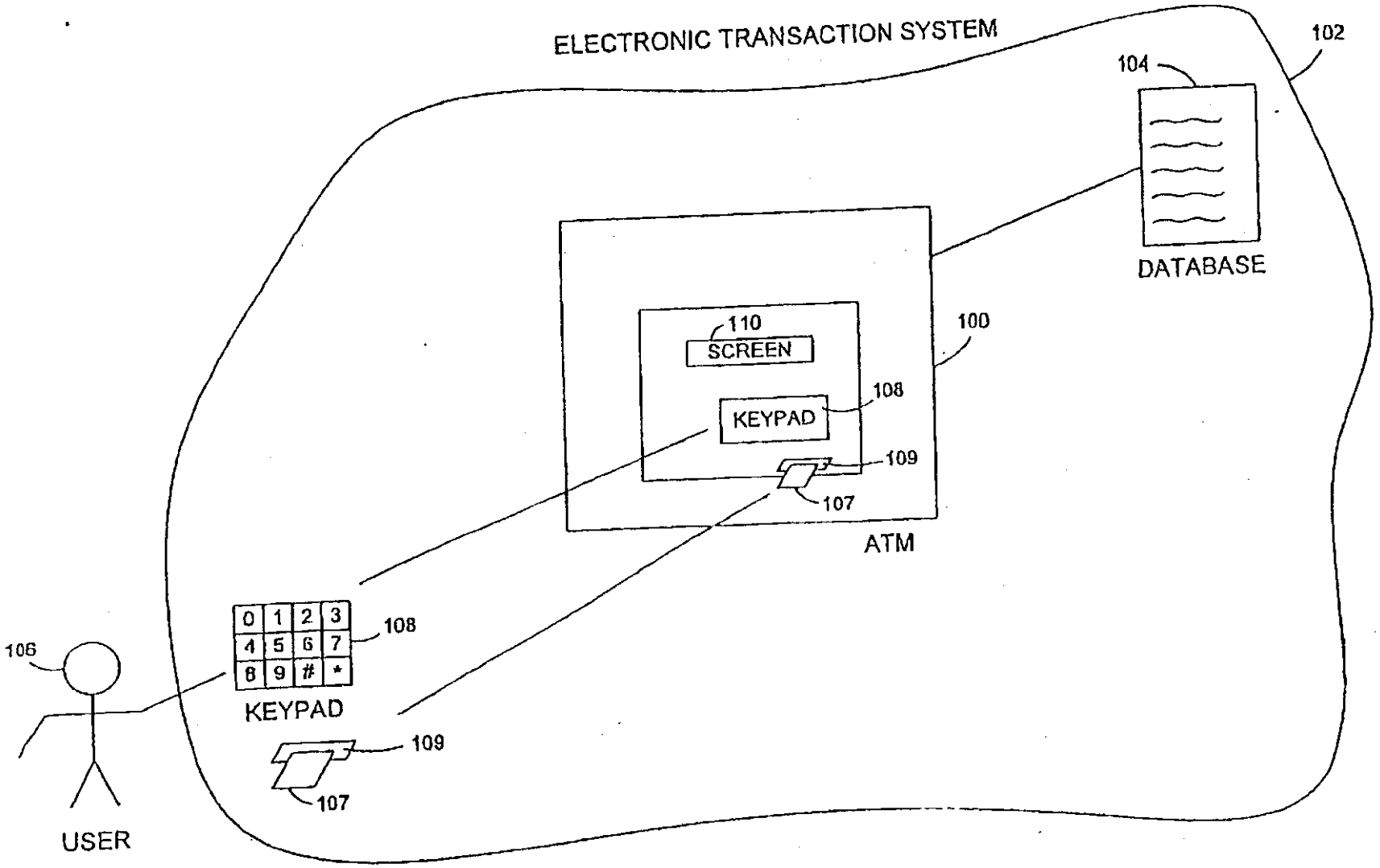


FIG. 1 (PRIOR ART)

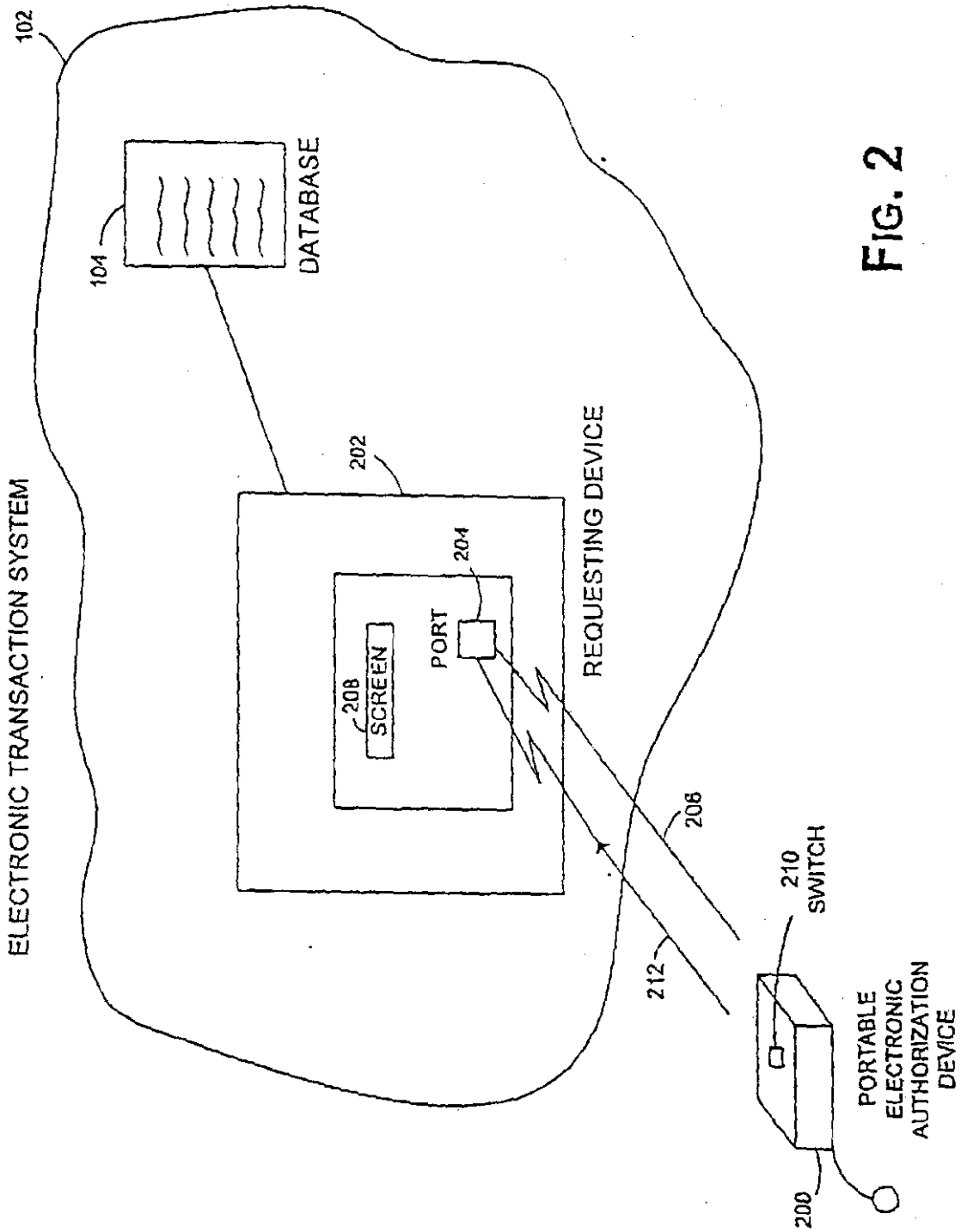

102
ELECTRONIC TRANSACTION SYSTEM
104
DATABASE
202
REQUESTING DEVICE
204
PORT
208
SCREEN
206
210
SWITCH
212
200
PORTABLE ELECTRONIC AUTHORIZATION DEVICE

FIG. 2

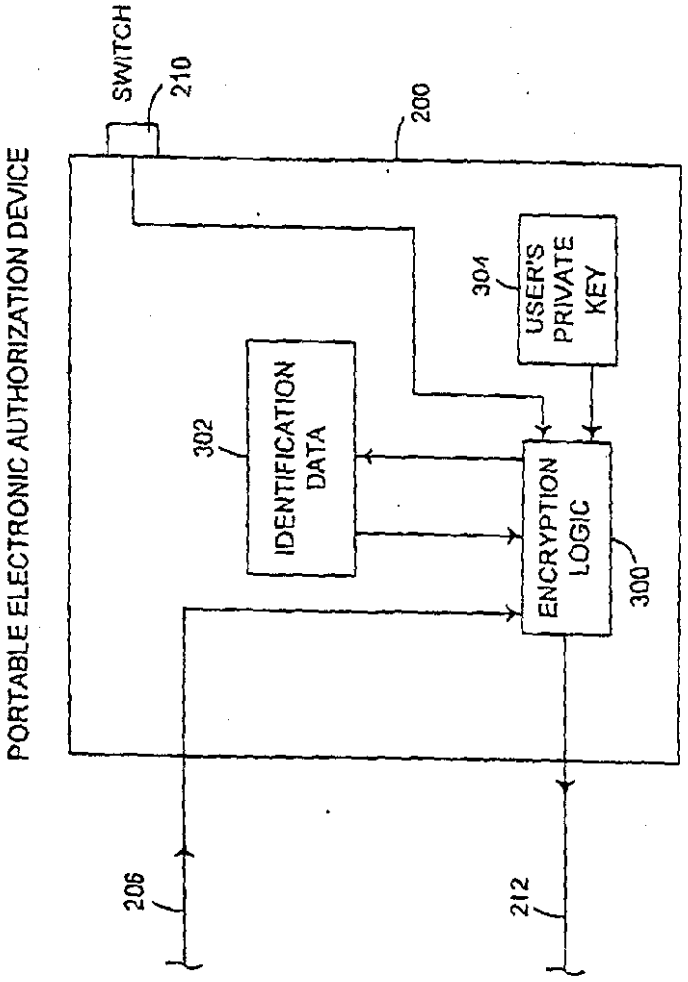

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
SWITCH
210
200
304
USER'S PRIVATE KEY
302
IDENTIFICATION DATA
ENCRYPTION LOGIC
300
206
212

FIG. 3A

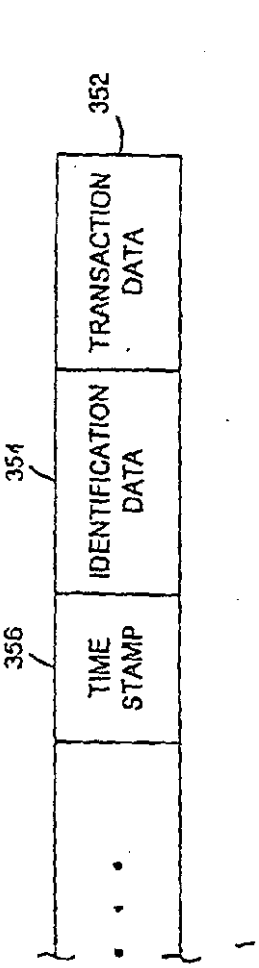

350
352
TRANSACTION DATA
354
IDENTIFICATION DATA
356
TIME STAMP

FIG. 3B

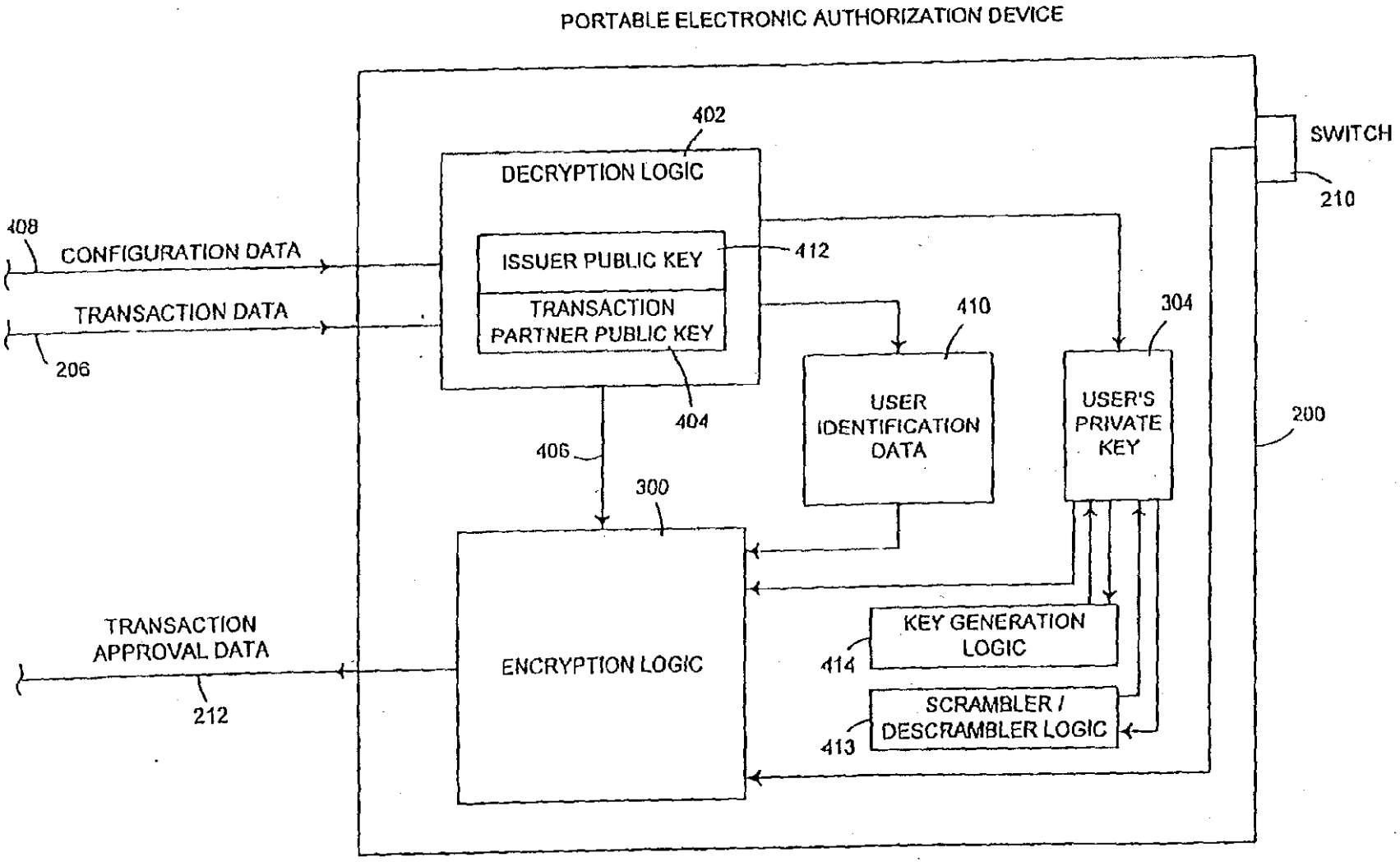

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
402
DECRYPTION LOGIC
SWITCH
210
408
CONFIGURATION DATA
ISSUER PUBLIC KEY
412
TRANSACTION DATA
TRANSACTION PARTNER PUBLIC KEY
206
404
410
304
USER IDENTIFICATION DATA
USER'S PRIVATE KEY
200
406
300
TRANSACTION APPROVAL DATA
212
ENCRYPTION LOGIC
KEY GENERATION LOGIC
414
SCRAMBLER / DESCRAMBLER LOGIC
413

FIG. 4

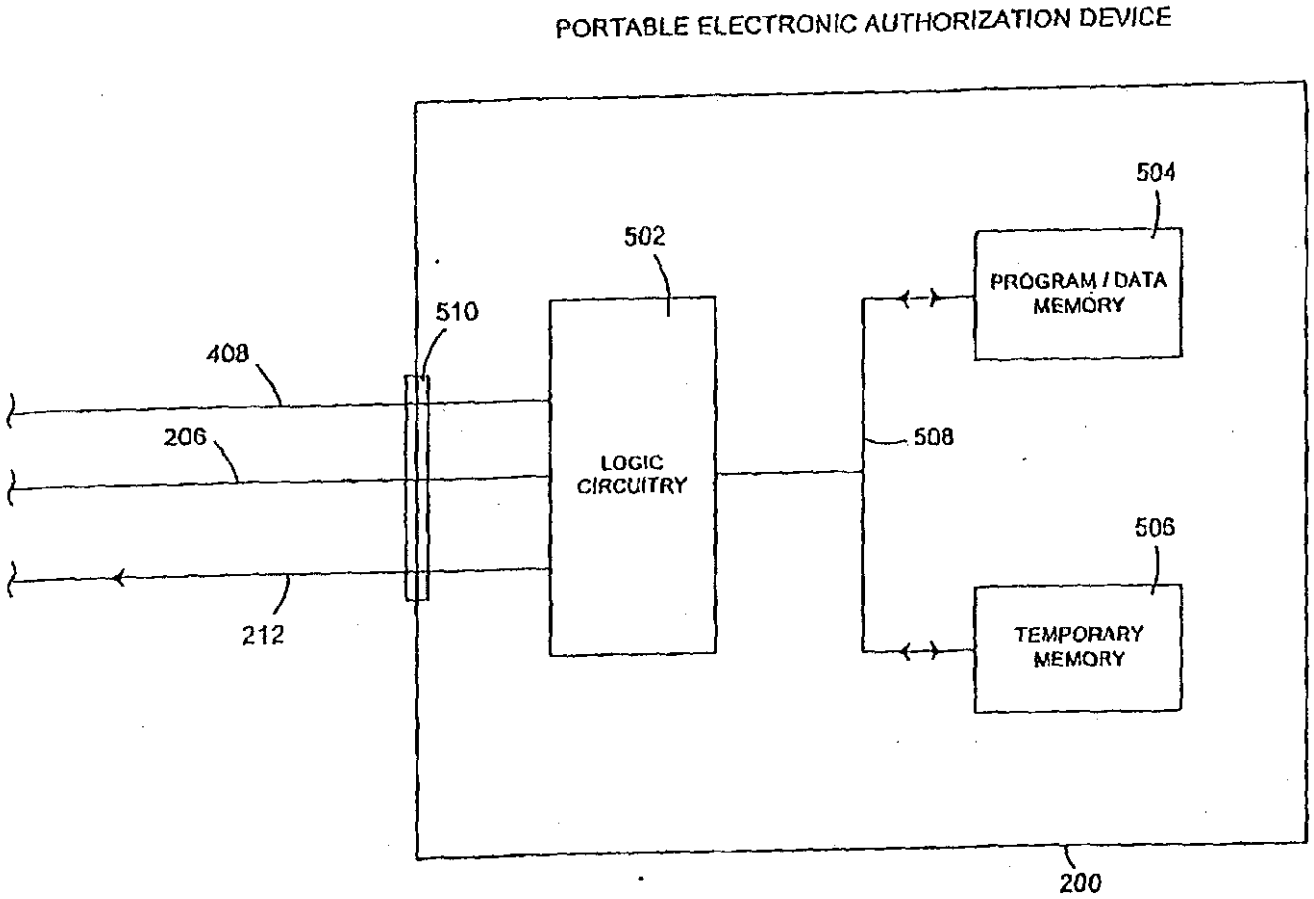

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
504
502
PROGRAM / DATA MEMORY
510
408
206
LOGIC CIRCUITRY
508
506
TEMPORARY MEMORY
212
200

FIG. 5A

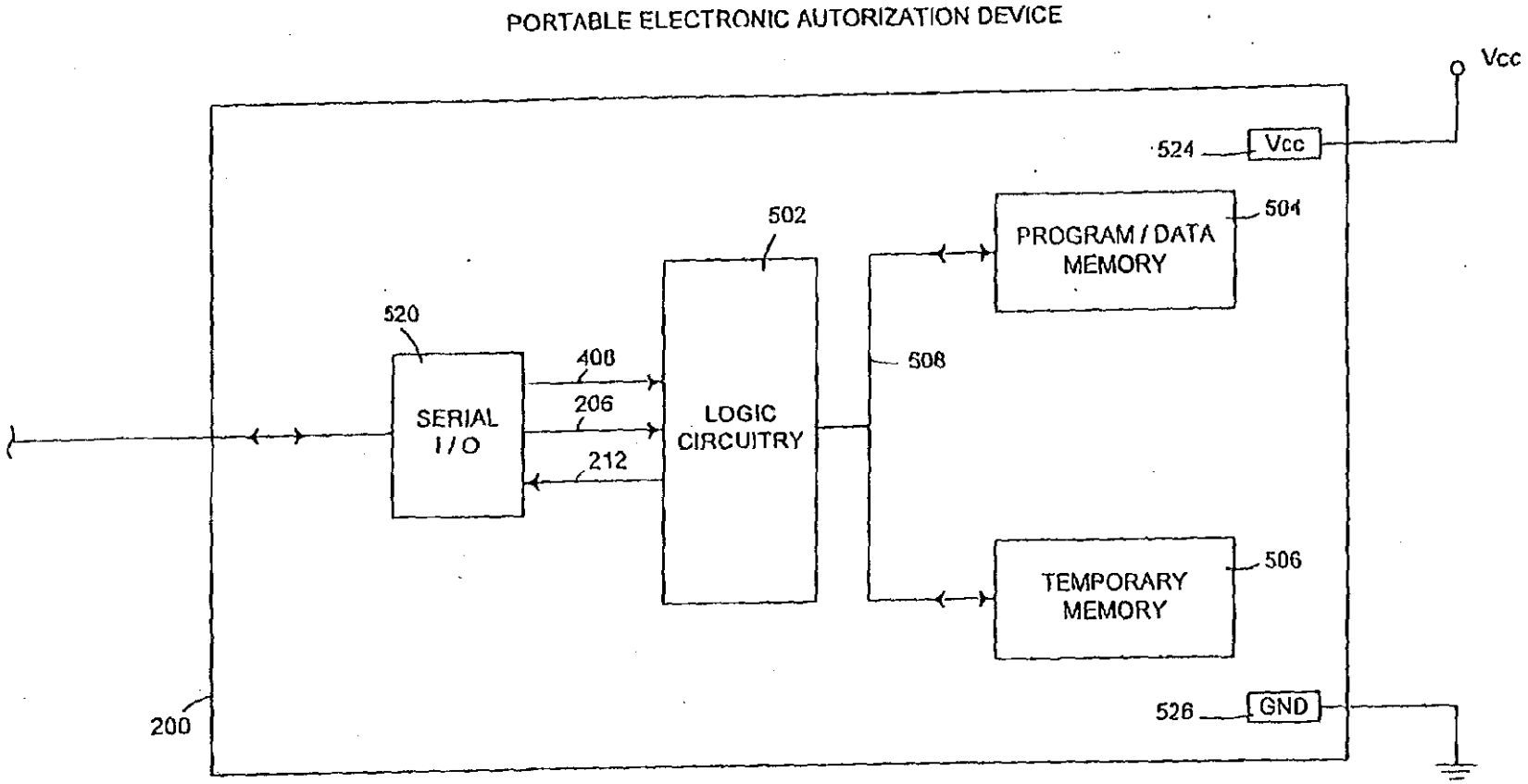

PORTABLE ELECTRONIC AUTORIZATION DEVICE
Vcc
524
Vcc
502
504
PROGRAM / DATA MEMORY
520
SERIAL I/O
408
206
212
LOGIC CIRCUITRY
508
TEMPORARY MEMORY
506
526
GND
200

FIG. 5B

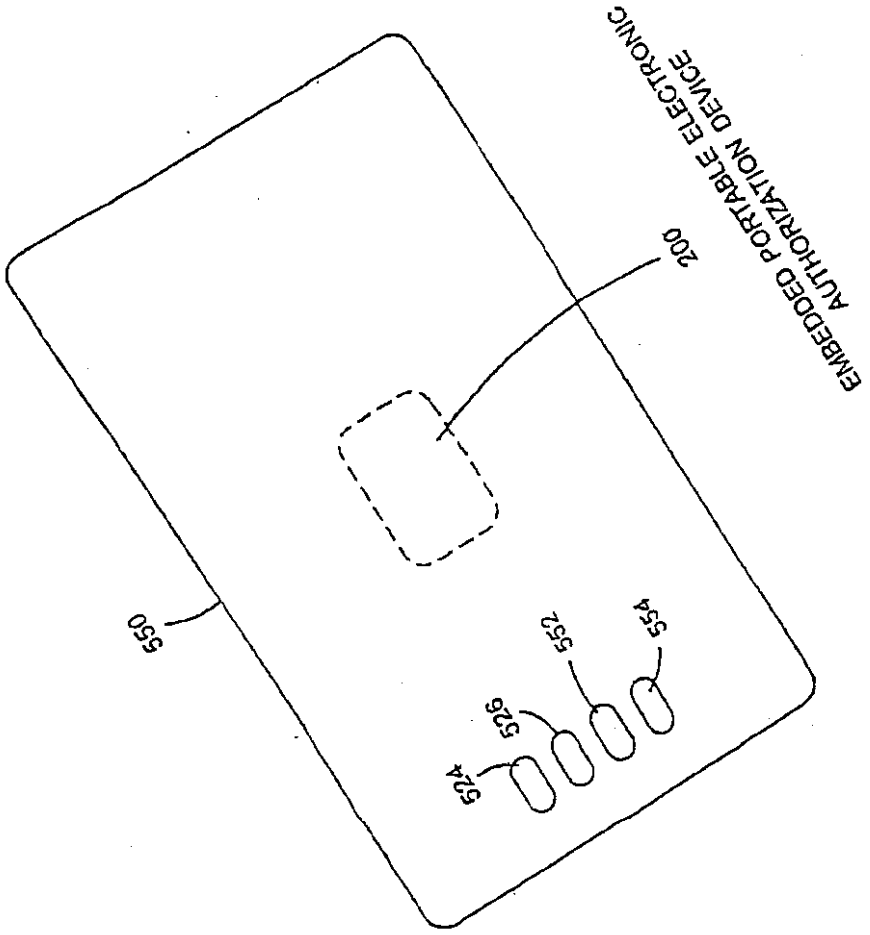

EMBEDDED PORTABLE ELECTRONIC AUTHORIZATION DEVICE
200
550
552
554
526
524

FIG. 5C

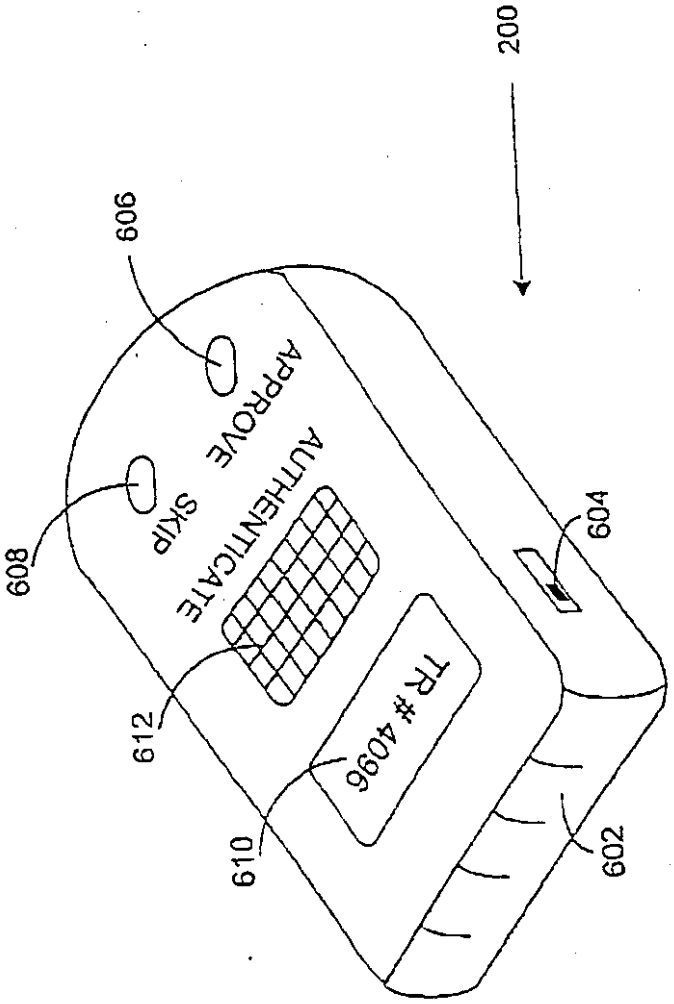

200
606
APPROVE
SKIP
608
AUTHENTICATE
604
612
TR # 4096
610
602

FIG. 6A

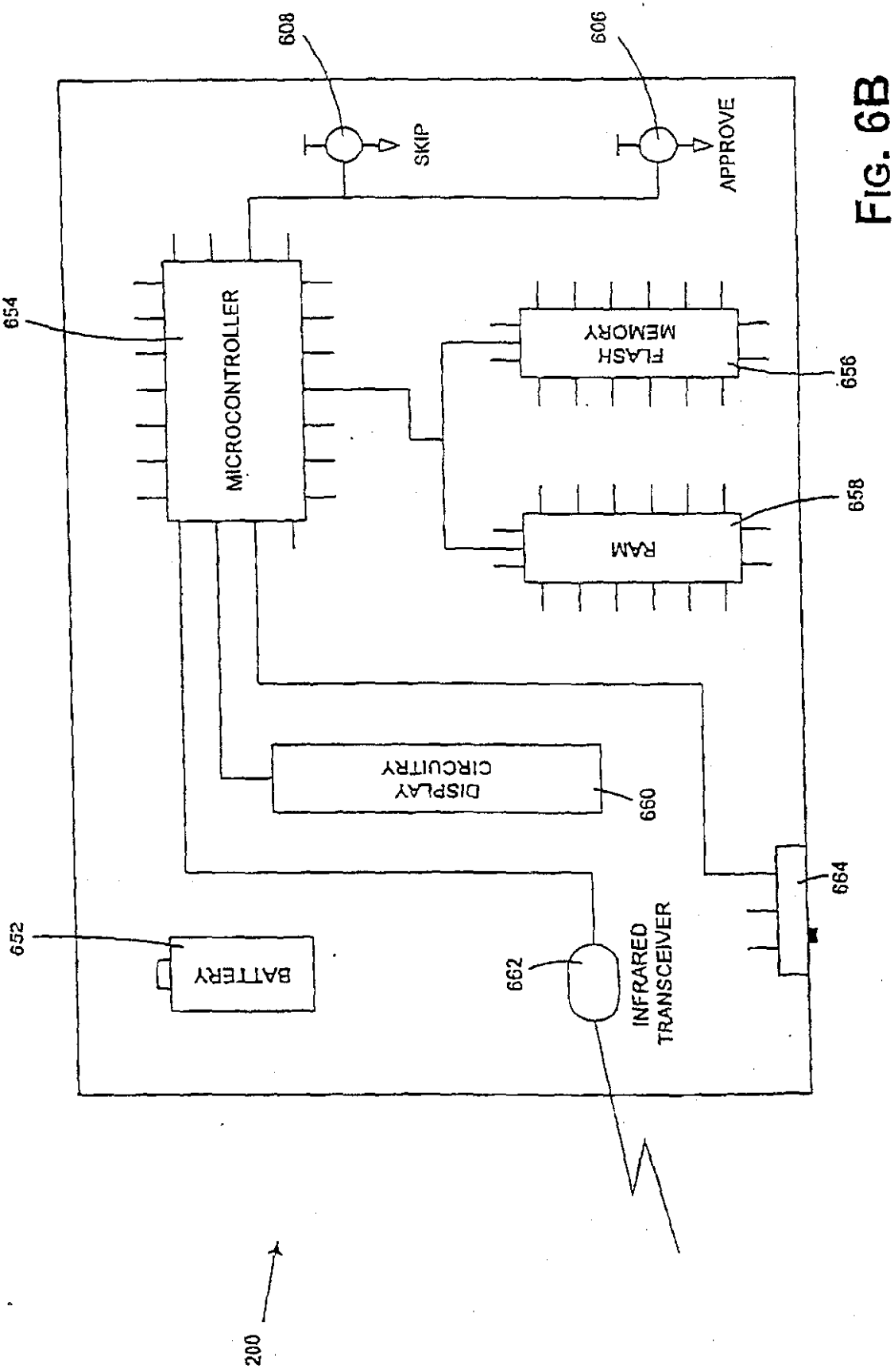

608
606
SKIP
APPROVE
654
MICROCONTROLLER
FLASH MEMORY
656
RAM
658
DISPLAY CIRCUITRY
660
664
652
BATTERY
662
INFRARED TRANSCEIVER
200

FIG. 6B

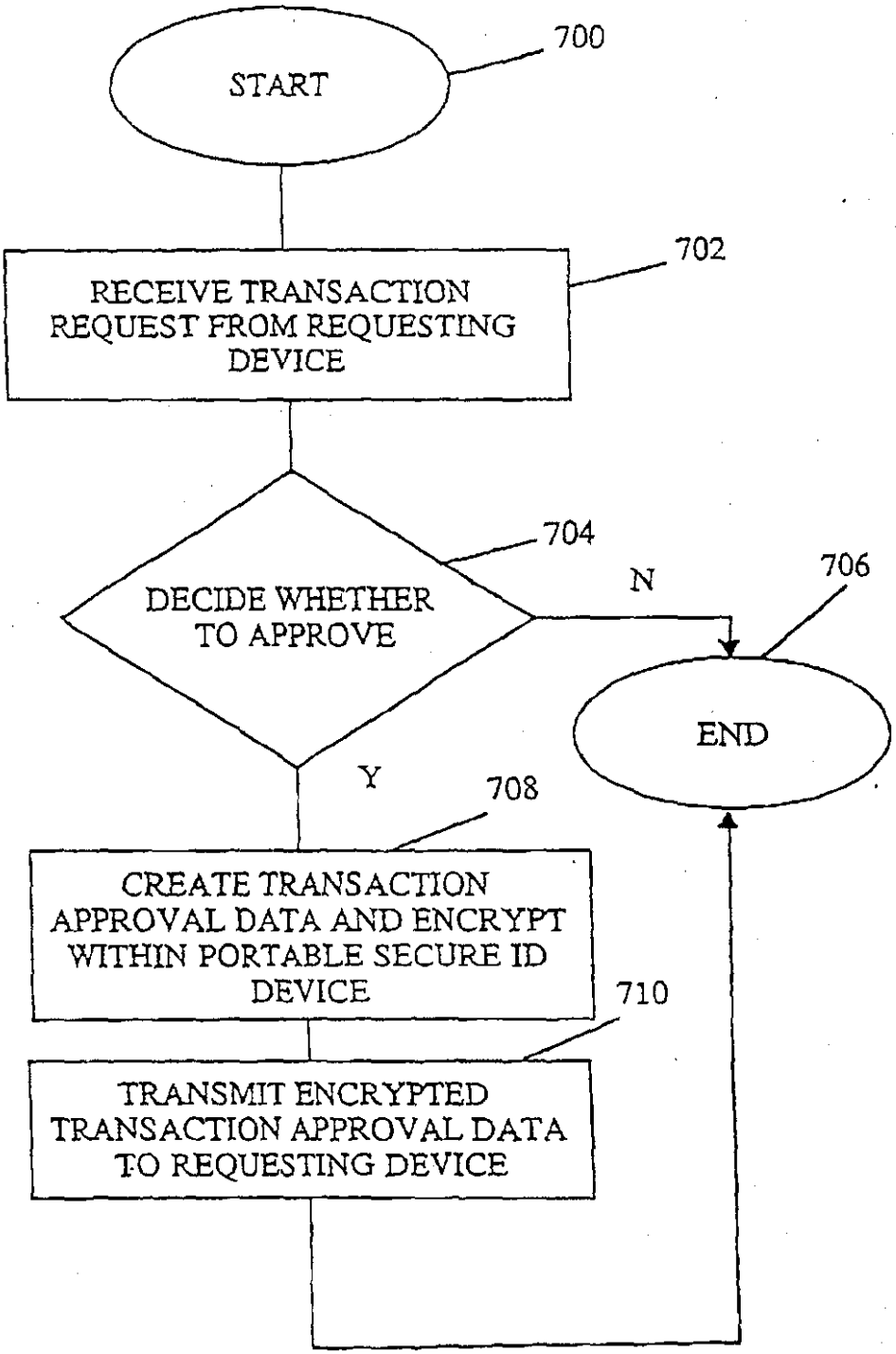

START
700
RECEIVE TRANSACTION REQUEST FROM REQUESTING DEVICE
702
DECIDE WHETHER TO APPROVE
704
N
706
END
Y
708
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT WITHIN PORTABLE SECURE ID DEVICE
710
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE

FIG. 7

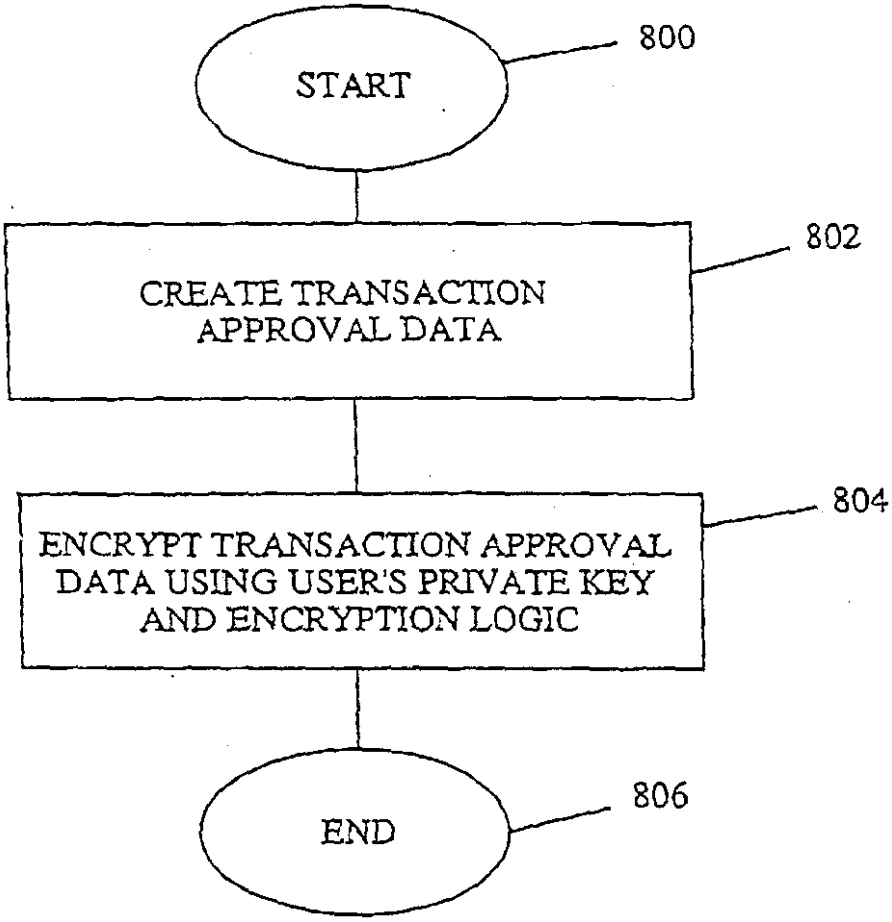

START
800
CREATE TRANSACTION APPROVAL DATA
802
ENCRYPT TRANSACTION APPROVAL DATA USING USER'S PRIVATE KEY AND ENCRYPTION LOGIC
804
END
806

FIG. 8

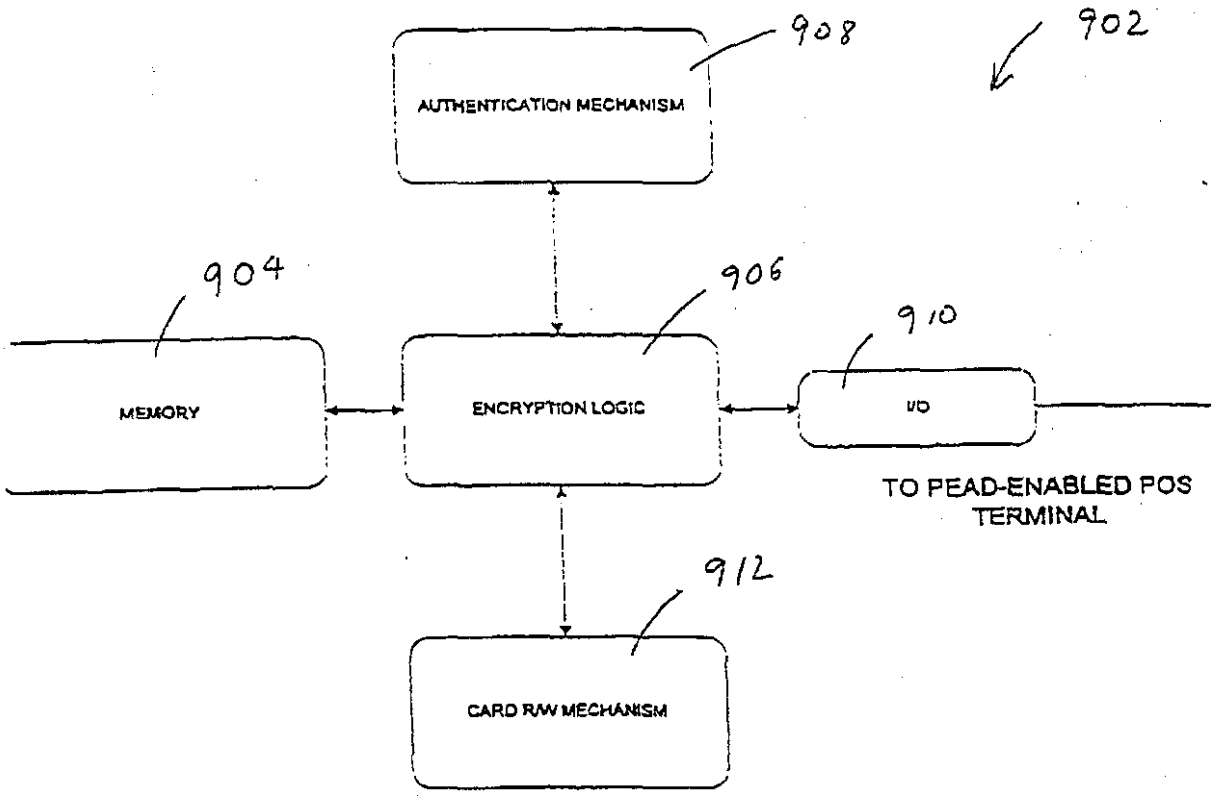

908
902
AUTHENTICATION MECHANISM
904
906
910
MEMORY
ENCRYPTION LOGIC
I/O
TO PEAD-ENABLED POS TERMINAL
912
CARD R/W MECHANISM

FIG. 9

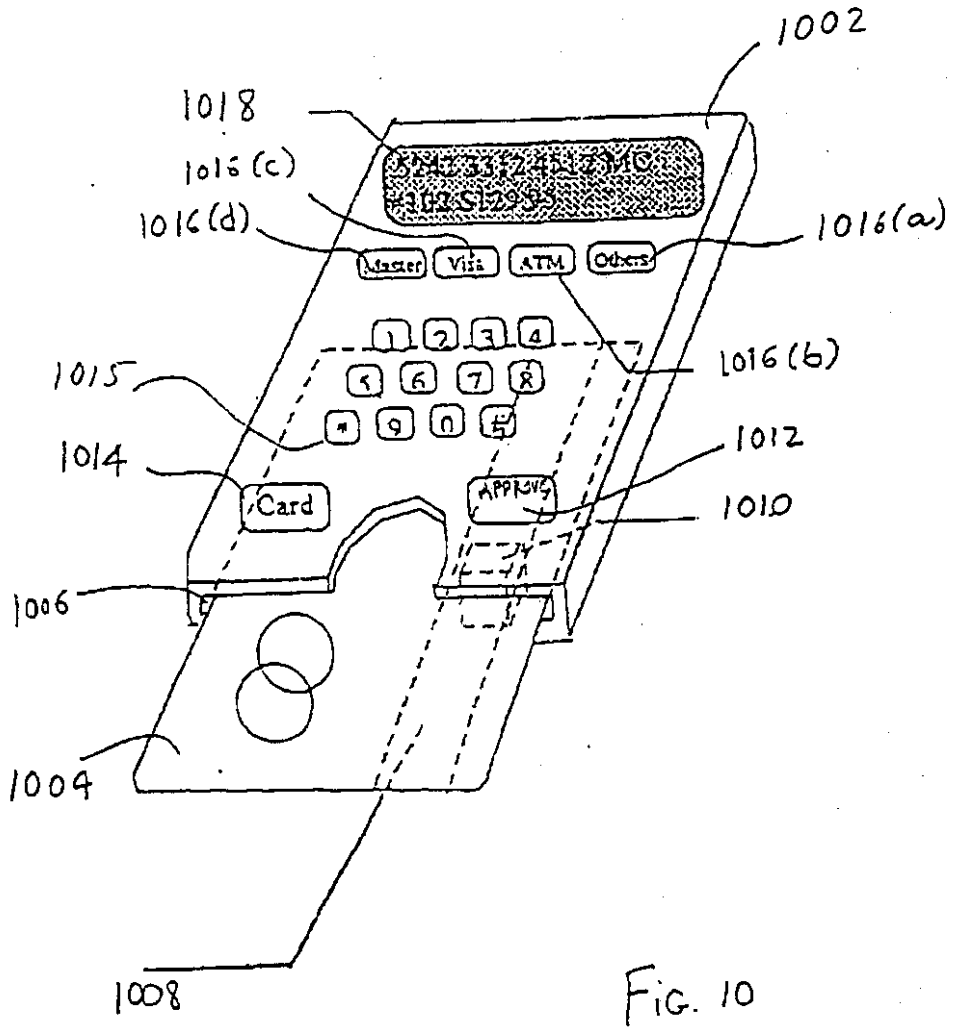

1002
1018
1016(c)
1016(d)
1016(a)
Master
Visa
ATM
Others
1016(b)
1015
1014
Card
1012
1010
1006
1004
1008

FIG. 10

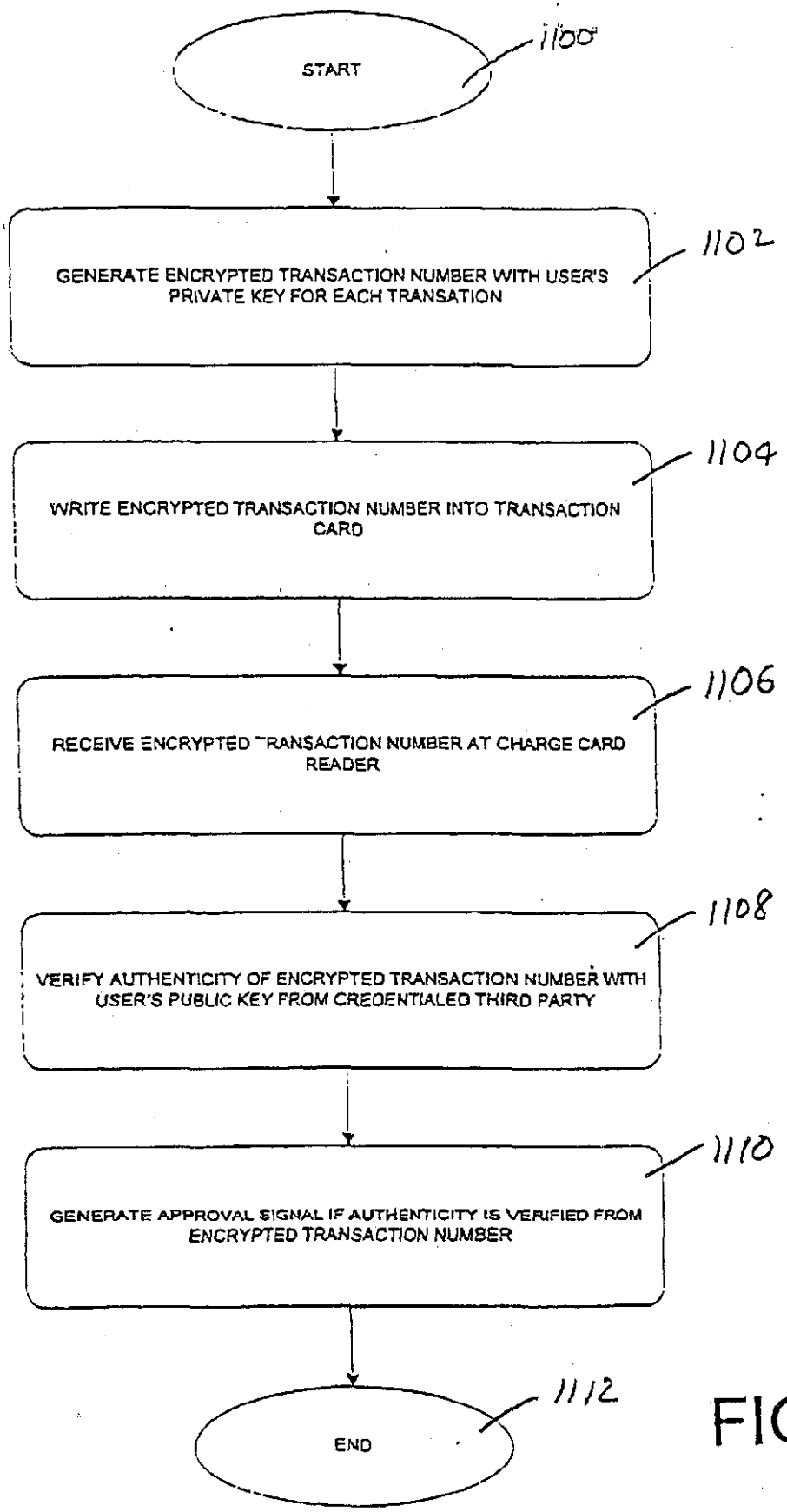

START
1100
GENERATE ENCRYPTED TRANSACTION NUMBER WITH USER'S PRIVATE KEY FOR EACH TRANSATION
1102
WRITE ENCRYPTED TRANSACTION NUMBER INTO TRANSACTION CARD
1104
RECEIVE ENCRYPTED TRANSACTION NUMBER AT CHARGE CARD READER
1106
VERIFY AUTHENTICITY OF ENCRYPTED TRANSACTION NUMBER WITH USER'S PUBLIC KEY FROM CREDENTIALED THIRD PARTY
1108
GENERATE APPROVAL SIGNAL IF AUTHENTICITY IS VERIFIED FROM ENCRYPTED TRANSACTION NUMBER
1110
END
1112

FIG. 11

參考檔號：DCSL/KKSW/6609541/5

(54) 標題：手提式電子收費及授權裝置及有關方法

(圖)

(57) 摘要：一個手提式交易裝置，可容許使用者(200)在一電子交易系統(102)的收費咭機進行一項交易。該收費咭機被配置成可與一收費咭溝通，以進行收費咭交易。該收費咭是磁帶咭及電子聰明咭。該手提式交易裝置包括一張含有模擬咭介面的模擬咭。該模擬咭介面模擬該收費咭的一個介面。收費咭的介面(202)使收費咭與收費咭機之間有更好的溝通。該裝置並包含一張可儲存使用者第一張收費咭數據的手提式模擬咭及一個鑑證系統。在使用者的身分被鑑定後，該手提式模擬咭將第一收費咭數據寫入模擬咭內，從而使模擬咭在寫入數據後透過模擬咭介面出現，並使收費咭機可從模擬咭中讀取第一收費咭的數據。