US 20020023215A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0023215 A1

Wang et al. (43) Pub. Date: Feb. 21, 2002

(54) ELECTRONIC TRANSACTION SYSTEMS AND METHODS THEREFOR

(76) Inventors: **Ynjiun P. Wang**, Cupertino, CA (US); **Joshua C. Ding**, San Jose, CA (US); **James A. Grizzard**, San Jose, CA (US)

Correspondence Address:
THOMASON, MOSER & PATTERSON, LLP
Suite B
4149 El Camino Way
Palo Alto, CA 94306-4036 (US)

(21) Appl. No.: **09/792,224**

(22) Filed: **Feb. 23, 2001**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/668,213, filed on Sep. 22, 2000, which is a continuation-in-part of application No. 09/523,825, filed on Mar. 13, 2000, now Pat. No. 6,175,922, which is a continuation-in-part of application No. 09/067,176, filed on Apr. 27, 1998, now Pat. No. 6,282,656, which is a continuation of application No. 08/759,555, filed on Dec. 4, 1996, now Pat. No. 5,917,913.

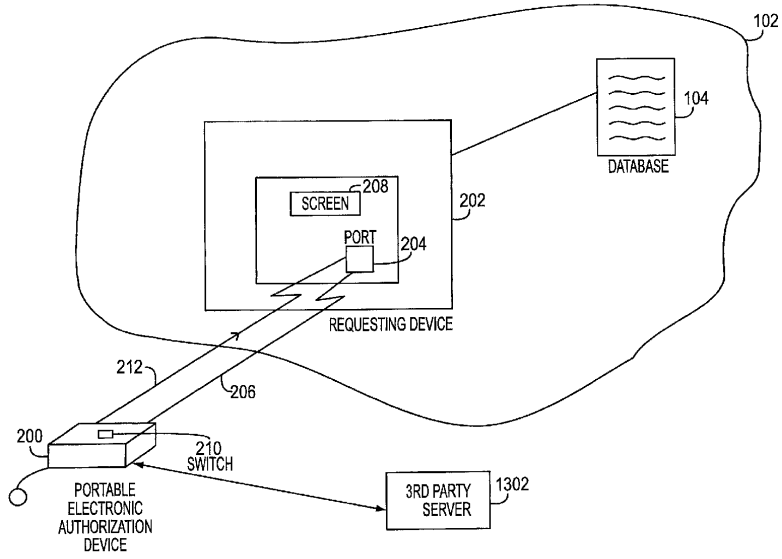
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**; H04K 1/00

(52) **U.S. Cl.** **713/171**; 713/184; 380/259; 380/277

(57) **ABSTRACT**

A method and apparatus are disclosed for approving a transaction request between an electronic transaction system and a portable electronic authorization device (PEAD) carried by a user using an electronic service authorization token. The method includes the steps of receiving at the PEAD first digital data representing the transaction request. The PEAD provides information to the user regarding an ability to approve the transaction request. When the transaction request is approved by the user, the PEAD receives second digital data representing the electronic service authorization token. In one aspect of the invention, the method and apparatus include a remote agent server that provides a bridge between the electronic transaction system and the PEAD. In an embodiment providing a further level of security, the private key is stored on the portable device, encrypted. The decryption key is stored outside of the device, at a trusted 3rd party location. When the user attempts to make a signature the software sends a request for the decryption key, along with the user's password or pass phrase keyed in at the keyboard of the PDA, smart phone, or cell phone, to a server belonging to the trusted 3rd party. This password is usually, but not always, different than the password stored in the PEAD. The server checks the password or pass phrase and, if it is correct sends the decryption key to the portable device, where it is used once and immediately discarded. In yet another aspect of the invention, the user's password is securely encoded in the method and apparatus and are used at a point-of-sale location. Advantages of the invention include the ability to securely and conveniently perform transactions in a portable device.



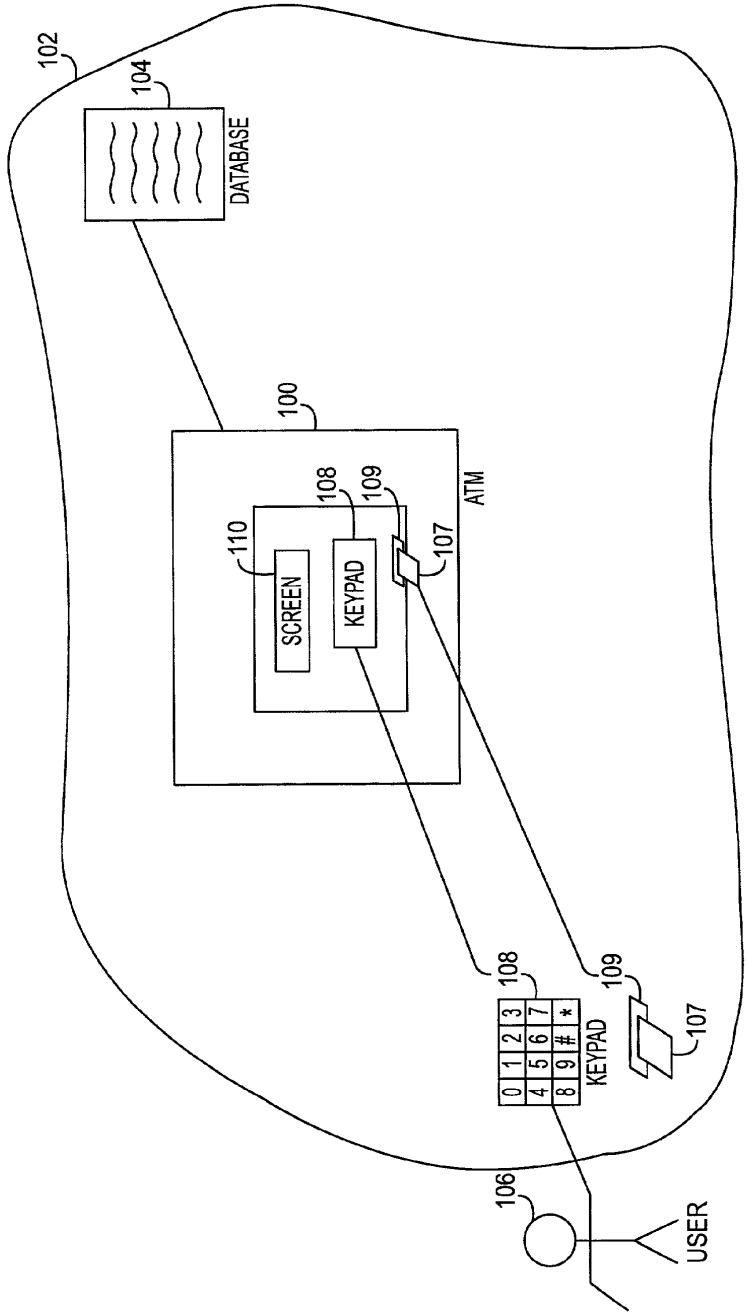


FIG. 1
(PRIOR ART)

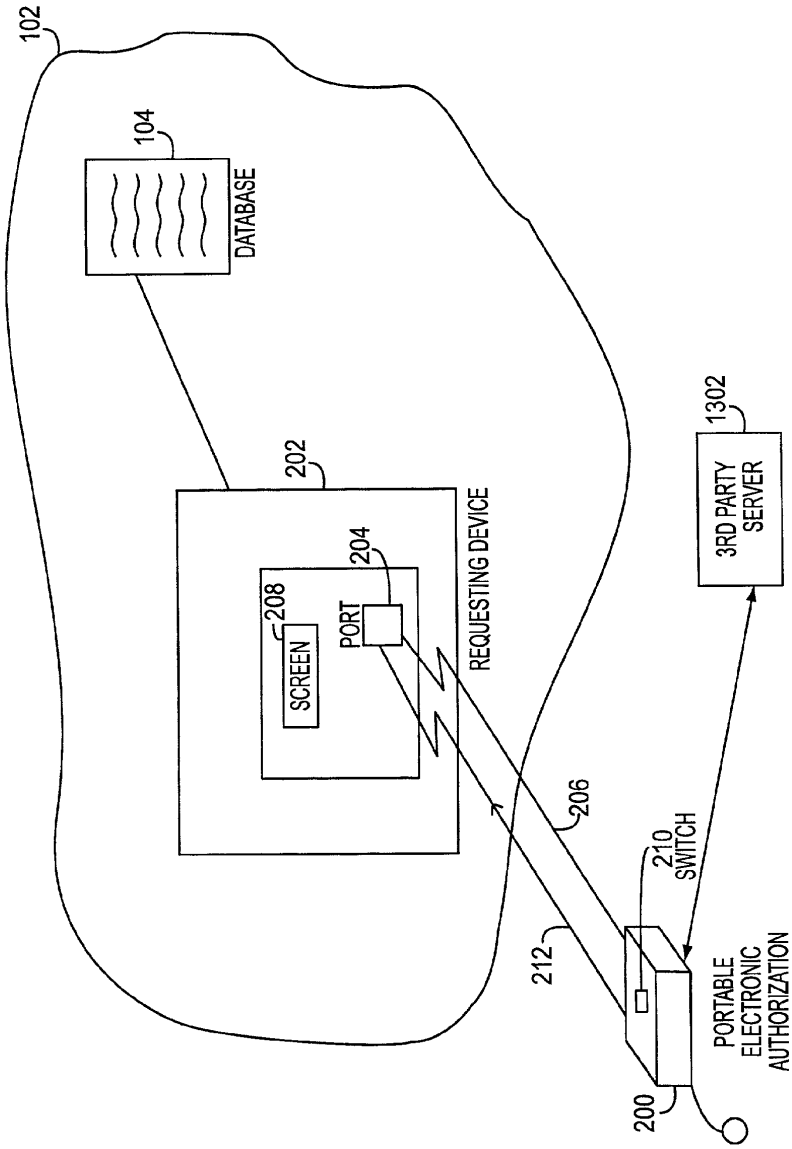

102
104
DATABASE
202
REQUESTING DEVICE
204
PORT
208
SCREEN
206
212
210
SWITCH
200
PORTABLE
ELECTRONIC
AUTHORIZATION
DEVICE
1302
3RD PARTY
SERVER

FIG. 2

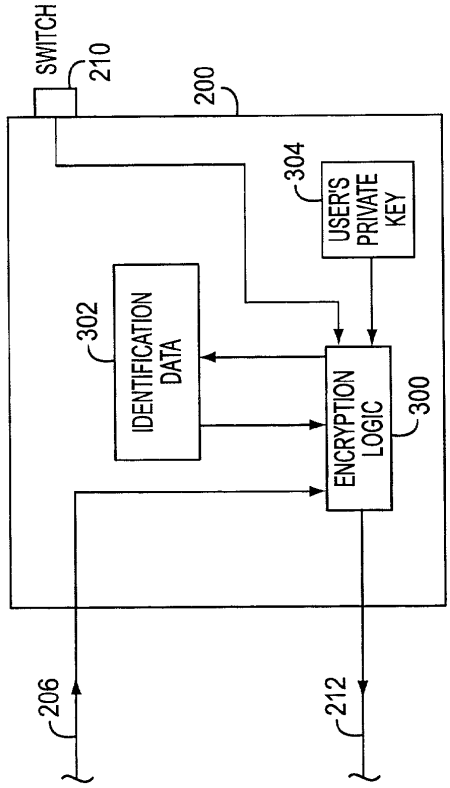


FIG. 3A

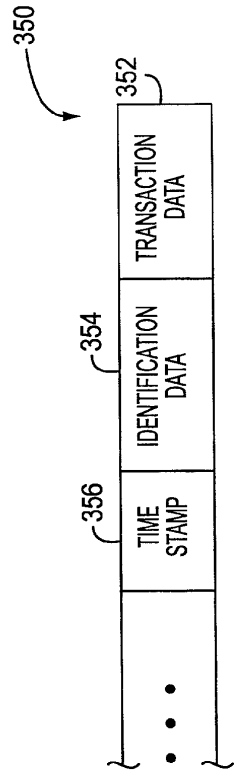


FIG. 3B

Early Warning
IPR2024-01221
Ex. 1004-4

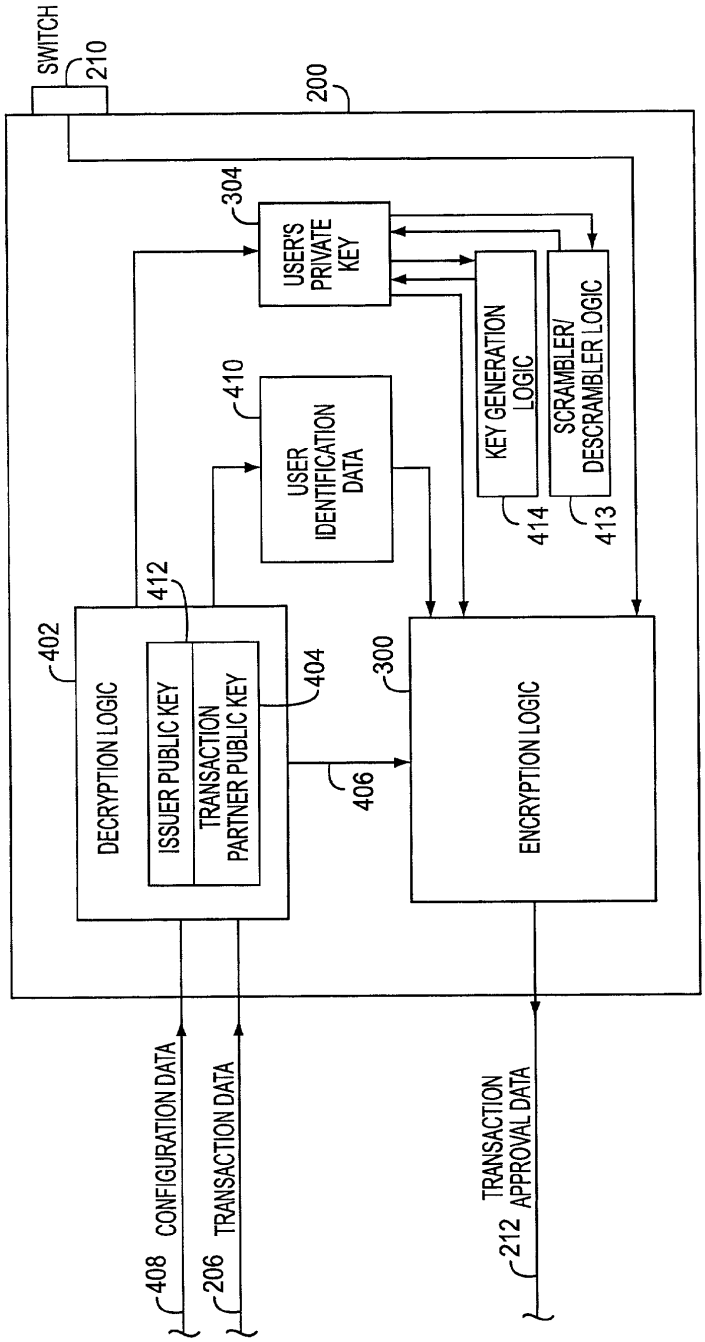

SWITCH
210
200
304
USER'S PRIVATE KEY
410
USER IDENTIFICATION DATA
KEY GENERATION LOGIC
SCRAMBLER/ DESCRAMBLER LOGIC
414
413
412
402
DECRYPTION LOGIC
ISSUER PUBLIC KEY
TRANSACTION PARTNER PUBLIC KEY
404
300
406
ENCRYPTION LOGIC
CONFIGURATION DATA
TRANSACTION DATA
TRANSACTION APPROVAL DATA
408
206
212

FIG. 4

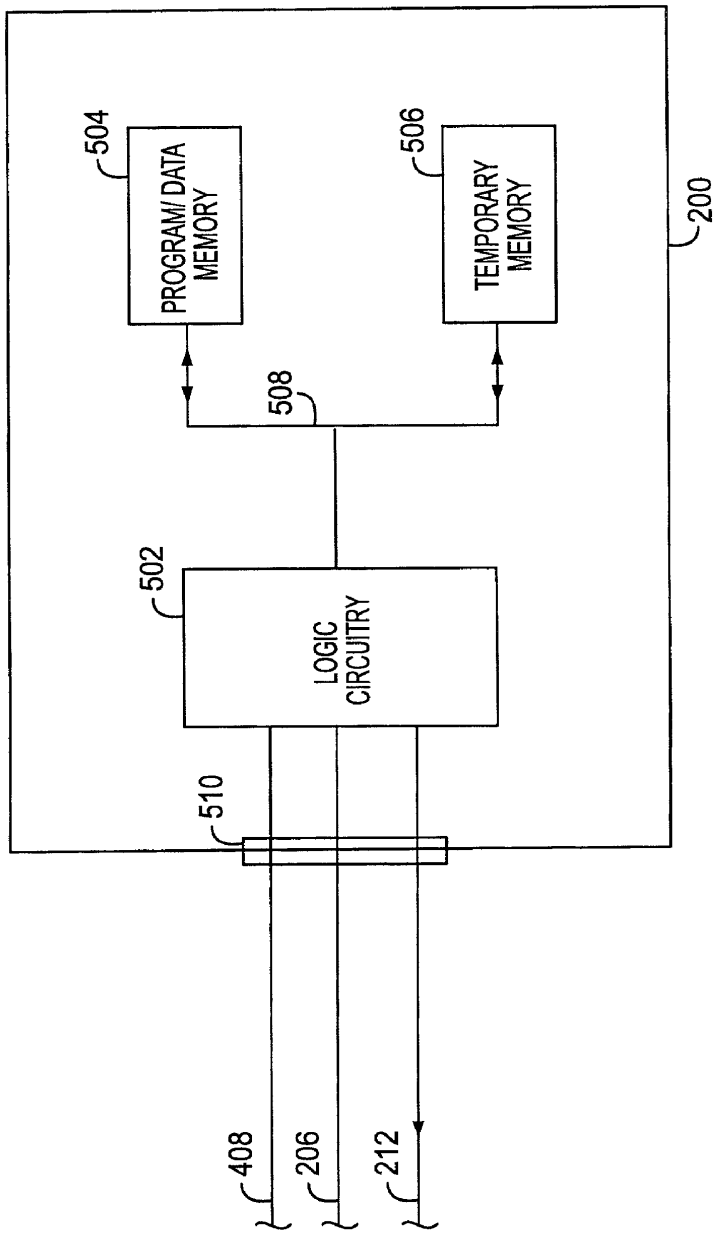

504
PROGRAM/ DATA MEMORY
506
TEMPORARY MEMORY
200
508
502
LOGIC CIRCUITRY
510
408
206
212

FIG. 5A

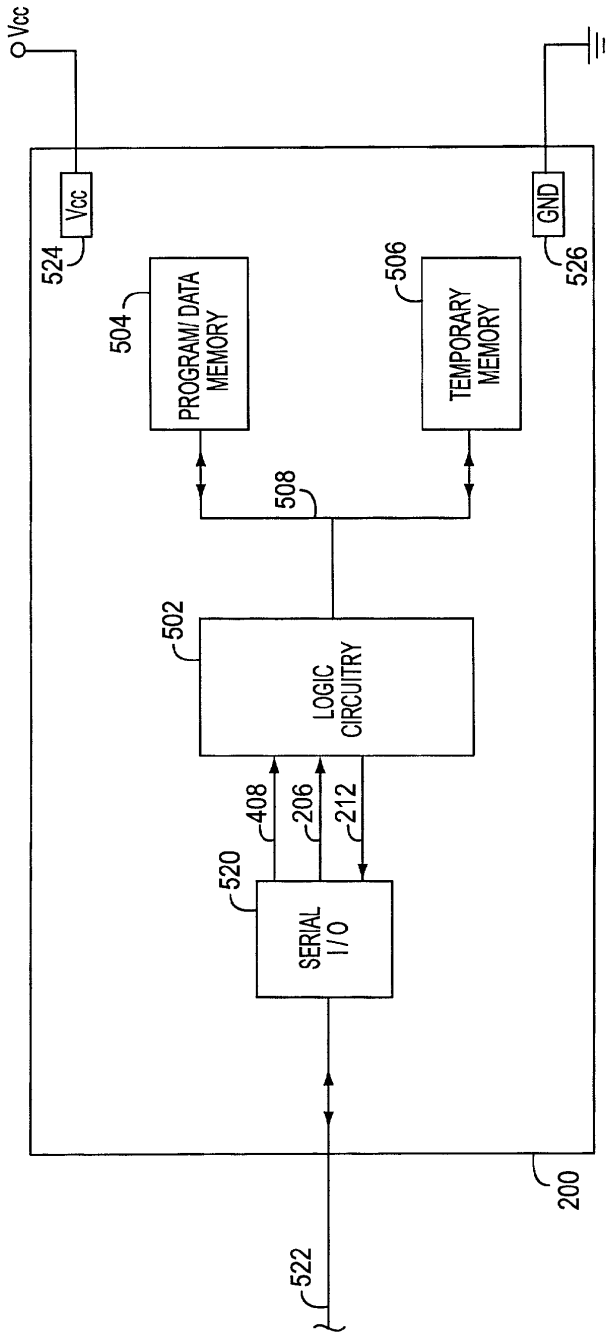

Vcc
524
Vcc
504
PROGRAM/ DATA MEMORY
506
TEMPORARY MEMORY
GND
526
508
502
LOGIC CIRCUITRY
408
206
212
520
SERIAL I/O
200
522

FIG. 5B

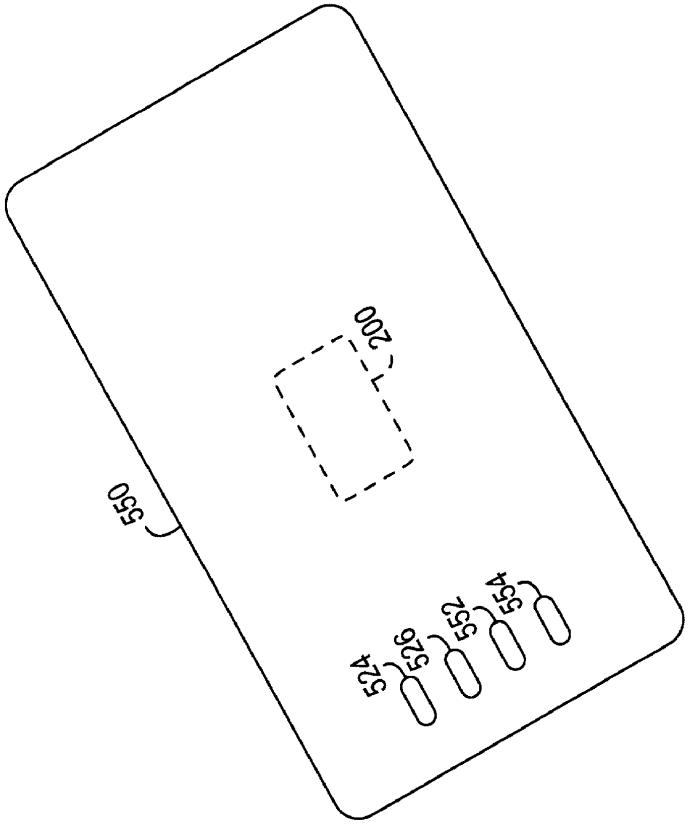


FIG. 5C

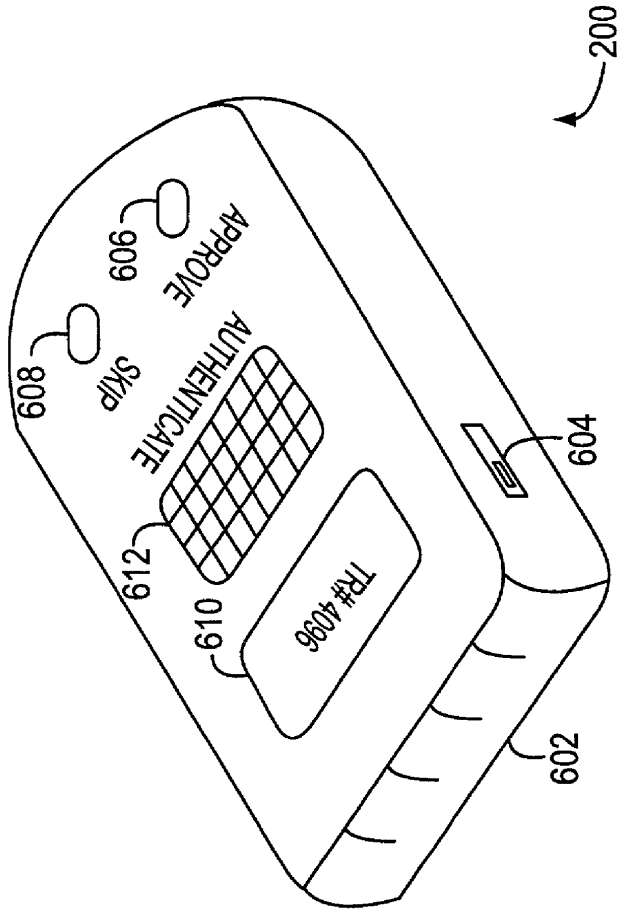

200
608
SKIP
606
APPROVE
AUTHENTICATE
612
610
TR#4096
604
602

FIG. 6A

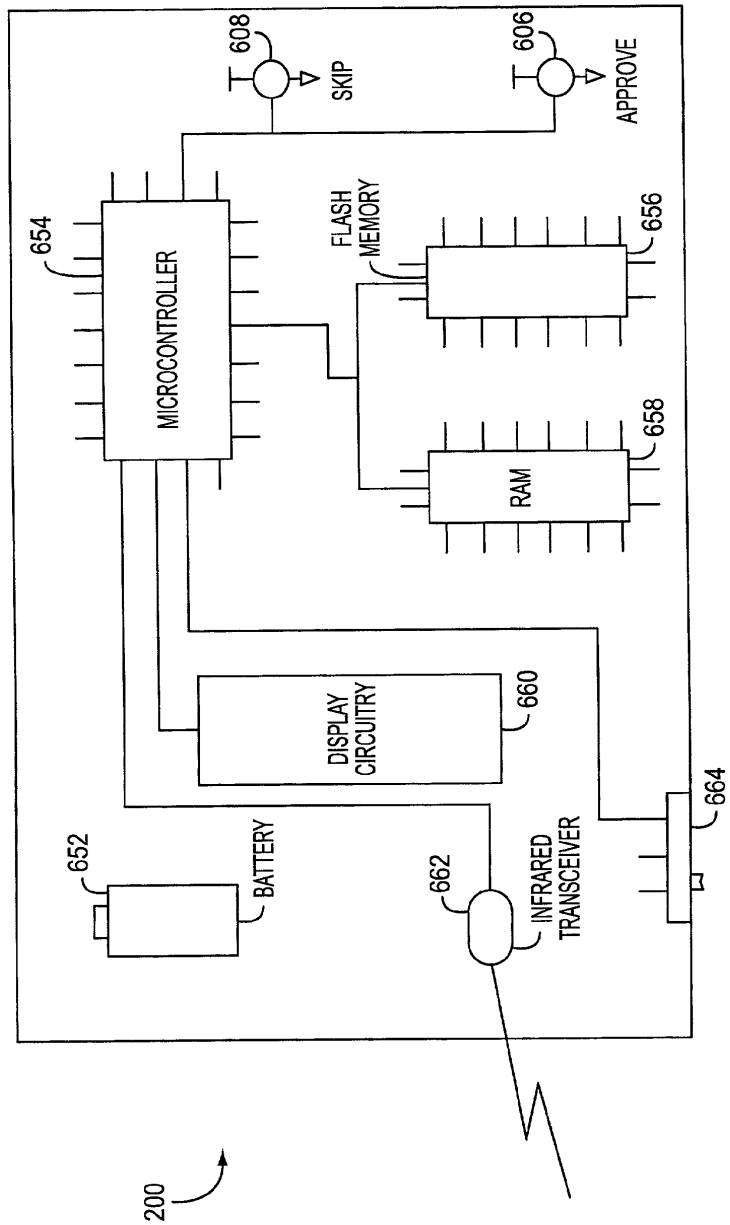

608
SKIP
606
APPROVE
654
MICROCONTROLLER
FLASH MEMORY
656
658
RAM
DISPLAY CIRCUITRY
660
652
BATTERY
662
INFRARED TRANSCEIVER
664
200

FIG. 6B

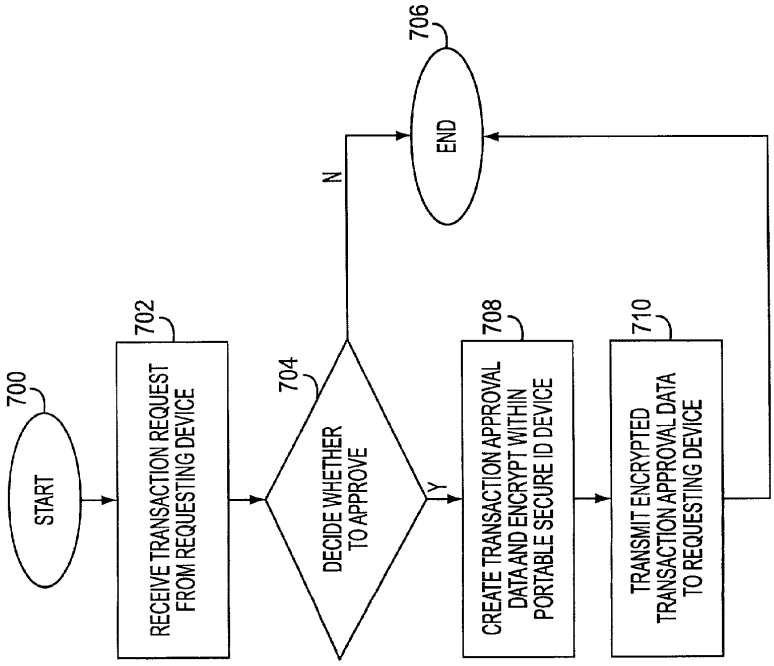

700
START
702
RECEIVE TRANSACTION REQUEST FROM REQUESTING DEVICE
704
DECIDE WHETHER TO APPROVE
N
Y
706
END
708
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT WITHIN PORTABLE SECURE ID DEVICE
710
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE

FIG. 7A

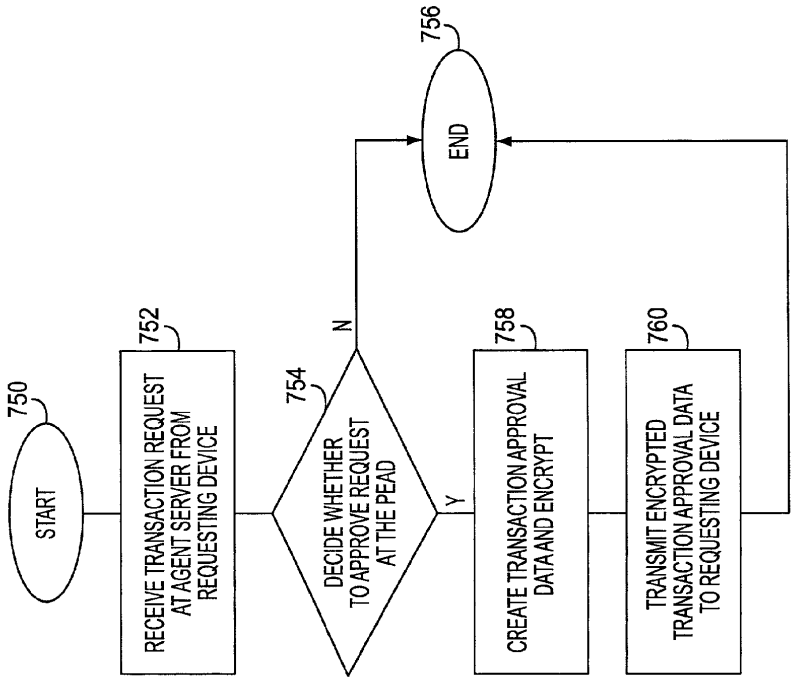

750
START
752
RECEIVE TRANSACTION REQUEST AT AGENT SERVER FROM REQUESTING DEVICE
754
DECIDE WHETHER TO APPROVE REQUEST AT THE PEAD
N
Y
756
END
758
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT
760
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE

FIG. 7B

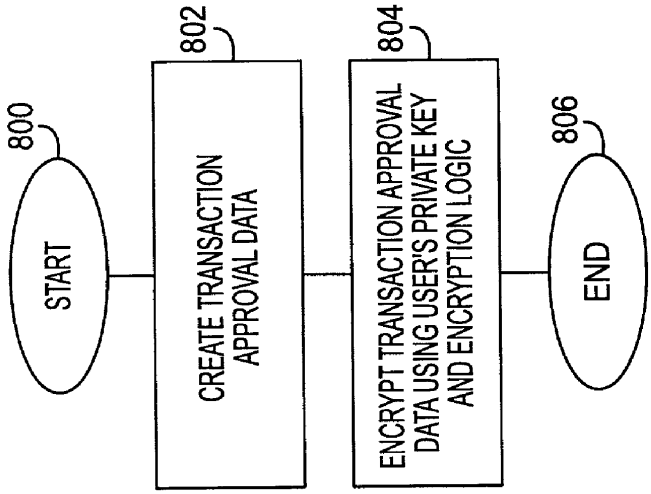

800
START
802
CREATE TRANSACTION APPROVAL DATA
804
ENCRYPT TRANSACTION APPROVAL DATA USING USER'S PRIVATE KEY AND ENCRYPTION LOGIC
806
END

FIG. 8

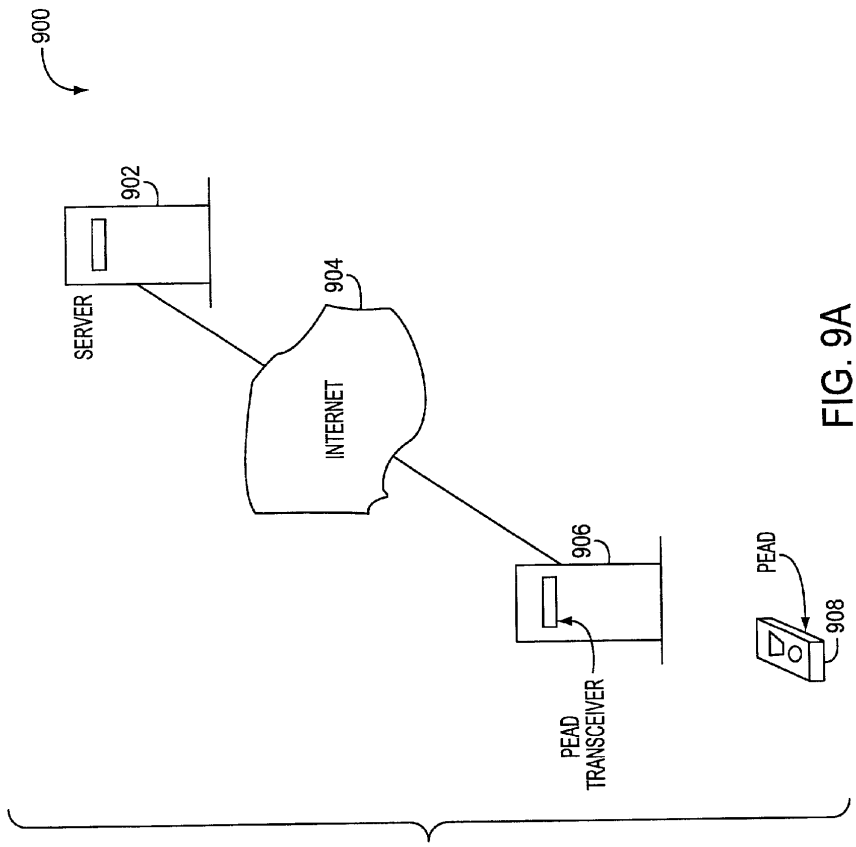


FIG. 9A

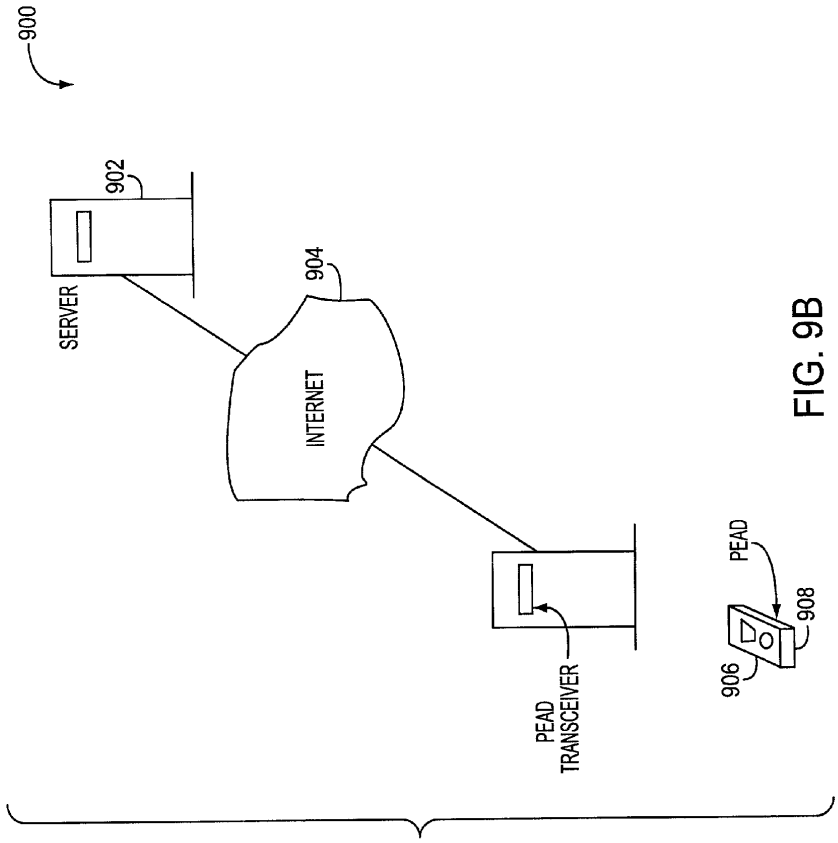


FIG. 9B

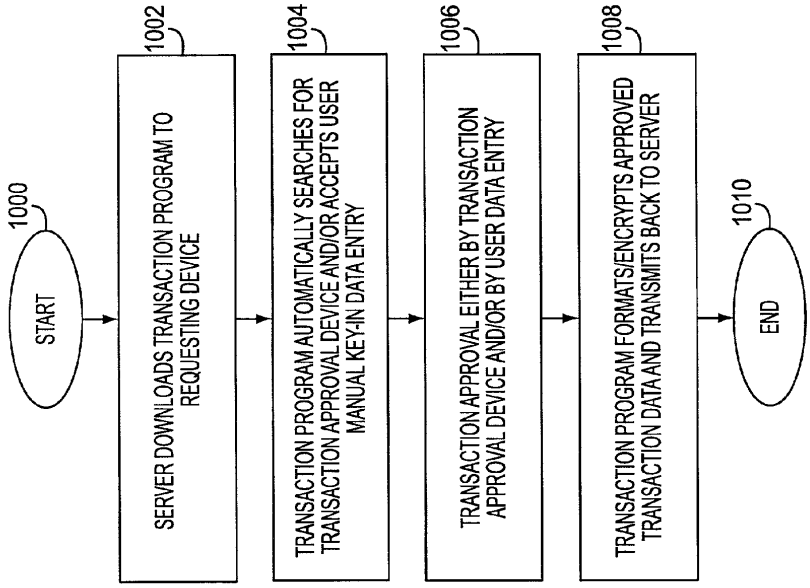

1000
START
1002
SERVER DOWNLOADS TRANSACTION PROGRAM TO REQUESTING DEVICE
1004
TRANSACTION PROGRAM AUTOMATICALLY SEARCHES FOR TRANSACTION APPROVAL DEVICE AND/OR ACCEPTS USER MANUAL KEY-IN DATA ENTRY
1006
TRANSACTION APPROVAL EITHER BY TRANSACTION APPROVAL DEVICE AND/OR BY USER DATA ENTRY
1008
TRANSACTION PROGRAM FORMATS/ENCRYPTS APPROVED TRANSACTION DATA AND TRANSMITS BACK TO SERVER
1010
END

FIG. 10

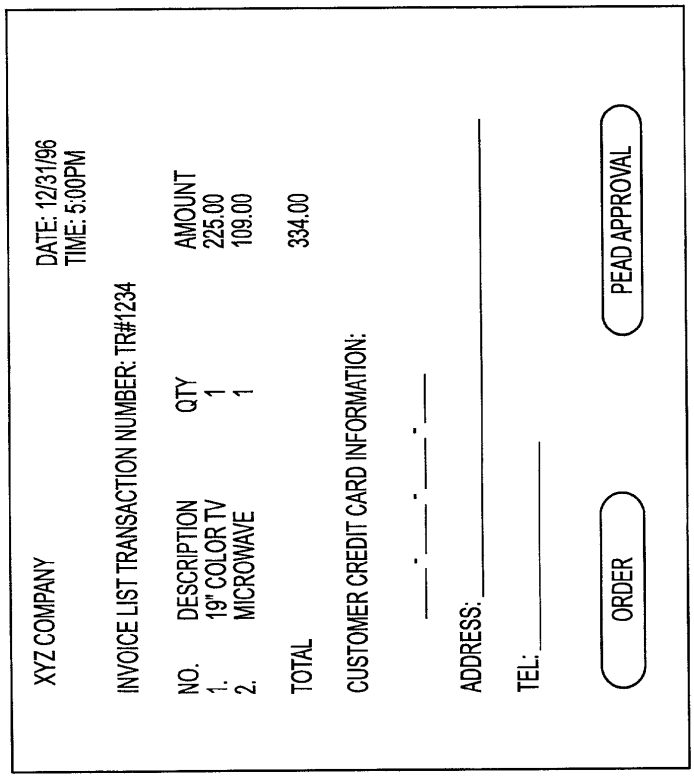

XYZ COMPANY
DATE: 12/31/96
TIME: 5:00PM
INVOICE LIST TRANSACTION NUMBER: TR#1234
NO. DESCRIPTION QTY AMOUNT
1. 19" COLOR TV 1 225.00
2. MICROWAVE 1 109.00
TOTAL 334.00
CUSTOMER CREDIT CARD INFORMATION:
___ - ___ - ___ - ___
ADDRESS: _____
TEL: _____
ORDER
PEAD APPROVAL

FIG. 11

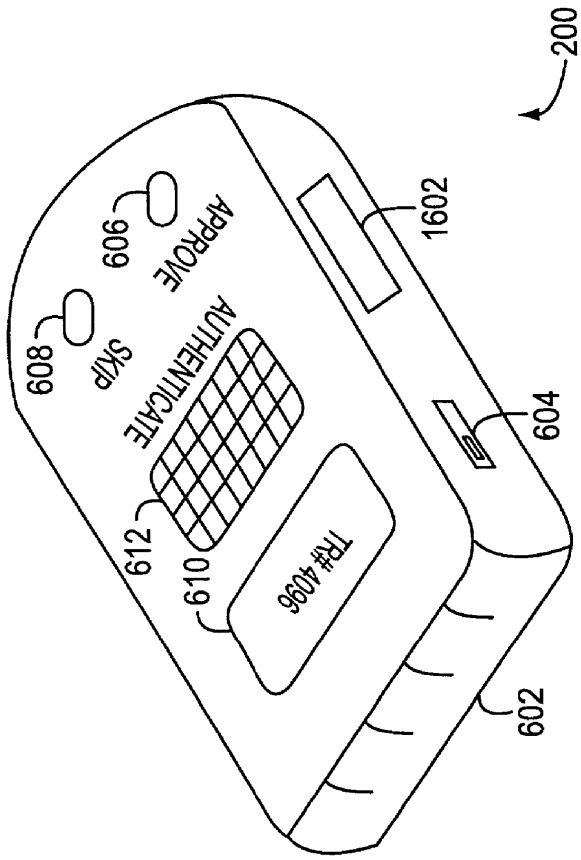


FIG. 12A

Early Warning
IPR2024-01221
Ex. 1004-18

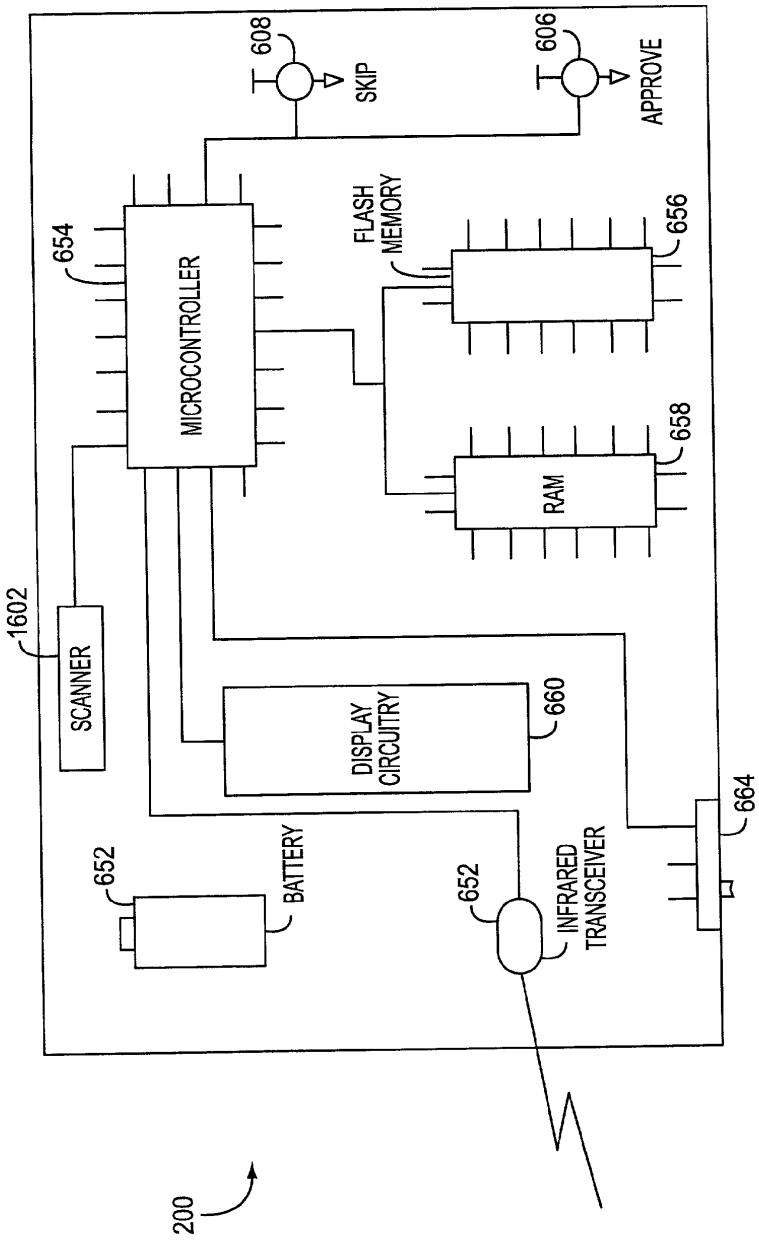

608
SKIP
606
APPROVE
654
MICROCONTROLLER
FLASH MEMORY
656
658
RAM
1602
SCANNER
DISPLAY CIRCUITRY
660
652
BATTERY
652
INFRARED TRANSCEIVER
664
200

FIG. 12B

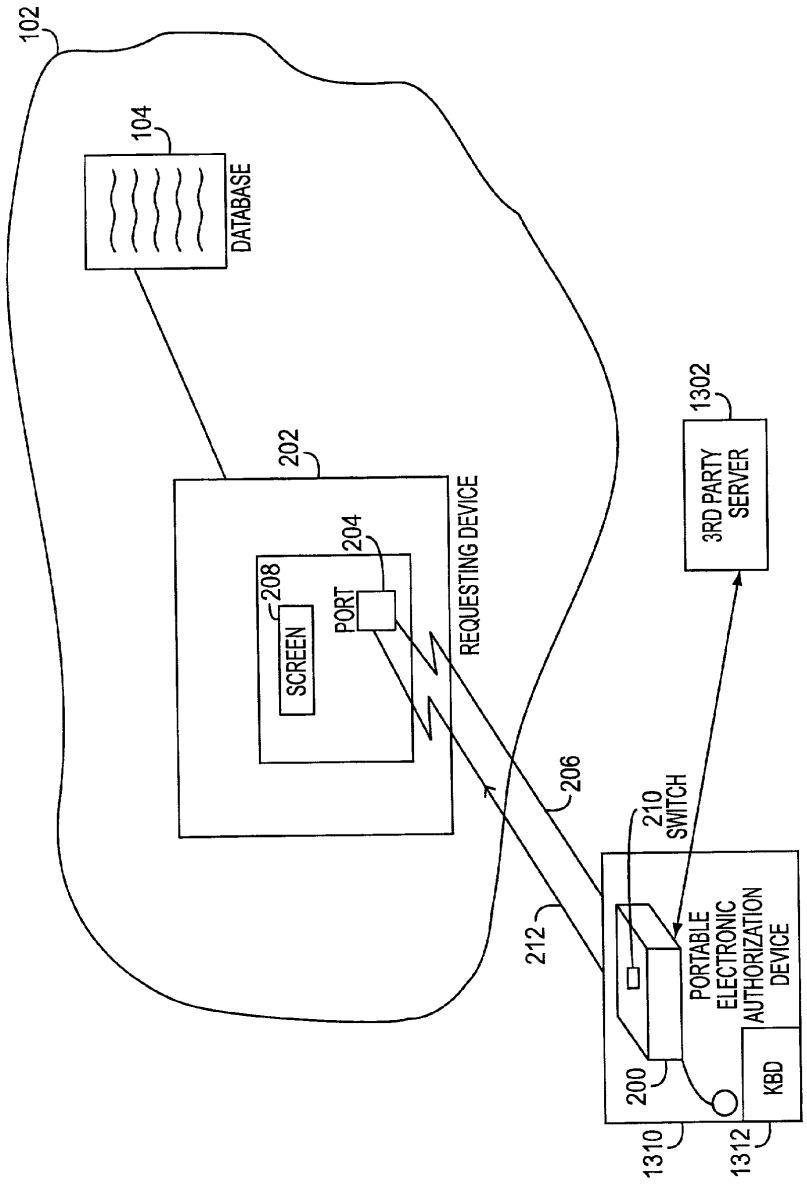

102
104
DATABASE
202
REQUESTING DEVICE
204
208
PORT
SCREEN
206
212
1302
3RD PARTY SERVER
210
SWITCH
PORTABLE ELECTRONIC AUTHORIZATION DEVICE
200
KBD
1310
1312

FIG. 13A

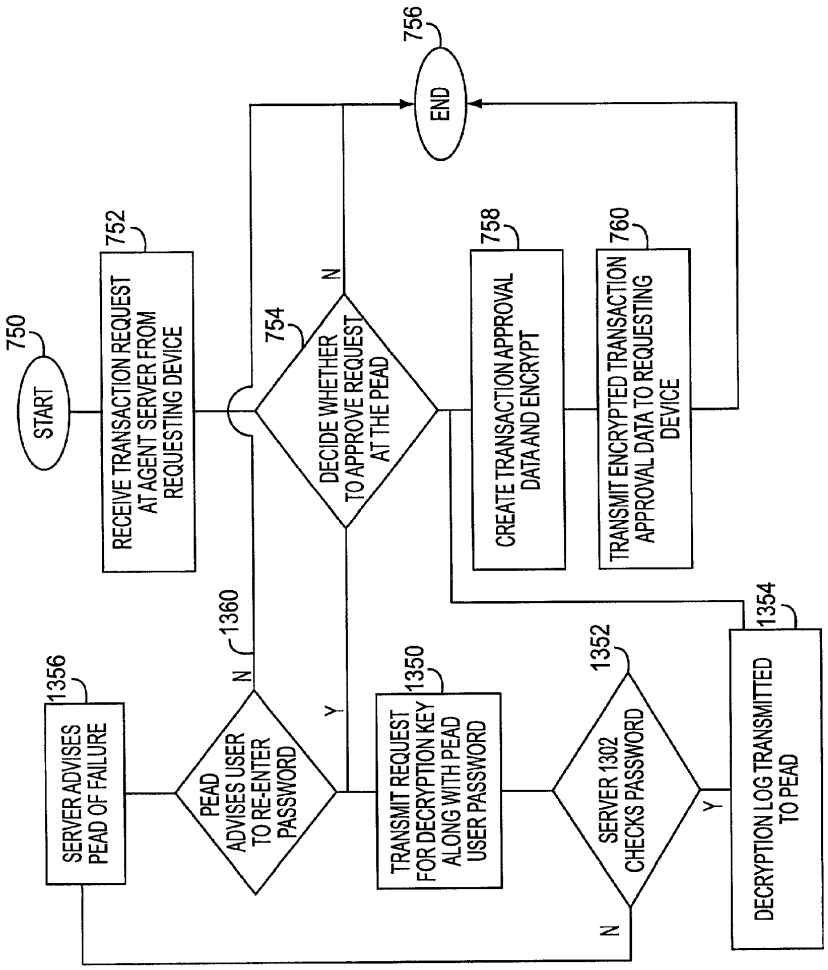

750
START
752
RECEIVE TRANSACTION REQUEST AT AGENT SERVER FROM REQUESTING DEVICE
754
DECIDE WHETHER TO APPROVE REQUEST AT THE PEAD
N
Y
756
END
758
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT
760
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE
1356
SERVER ADVISES PEAD OF FAILURE
1360
PEAD ADVISES USER TO RE-ENTER PASSWORD
N
Y
1350
TRANSMIT REQUEST FOR DECRYPTION KEY ALONG WITH PEAD USER PASSWORD
1352
SERVER 1302 CHECKS PASSWORD
N
Y
1354
DECRYPTION LOG TRANSMITTED TO PEAD

FIG. 13B

ELECTRONIC TRANSACTION SYSTEMS AND METHODS THEREFOR

RELATED APPLICATIONS

[0001] This application is a continuation in part of U.S. Ser. No. 09/668,213 filed Sep. 22, 2000, which is a continuation in part of U.S. Ser. No. 09/523,825 filed Mar. 13, 2000, now U.S. Pat. No. 6,175,922, which is a continuation in part of U.S. Ser. No. 09/067,176 filed Apr. 27, 1998, which is a continuation of U.S. Ser. No. 08/759,555 filed Dec. 4, 1996 now U.S. Pat. No. 5,917,913.

BACKGROUND OF THE INVENTION

[0002] 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.

[0003] 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.

[0004] To enhance security to the user's account, electronic transaction systems typically request the user to provide identification data to authenticate him 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 him and enable that user to subsequently perform any number of transactions without further authentication.

[0005] 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.

[0006] 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**.

[0007] To initiate a typical transaction with ATM **100**, user **106** first inserts a data card **107**, such as a bankcard 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.

[0008] 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 not 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.

[0009] 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**.

[0010] 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

Early Warning
IPR2024-01221
Ex. 1004-22

100 and intercepts, e.g., via software or hardware implemented in ATM **100**, the non-encrypted identification data therein.

[**0011**] 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.

[**0012**] 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

[**0013**] The present invention relates, in one embodiment, to a method for completing a transaction request pertaining to an electronic transaction conducted over an electronic network having a server and a requesting device and including steps to provide an enhanced level of security. The method includes receiving from the server at the requesting device a transaction program, which includes an executable portion. The method also includes searching, employing the executable portion, for a transaction approval device associated with the requesting terminal. If the transaction approval device is detected, the method includes employing the transaction approval device to approve the transaction request. There is further included transmitting, using the requesting device, an approved transaction request to the server to complete the electronic transaction. The approved transaction request signifies an approval of the transaction request.

[**0014**] In another embodiment, the invention relates to a method for completing a transaction request pertaining to an electronic transaction conducted over an electronic network having a server and a requesting device. The method includes receiving from the server at the requesting device a transaction program, which includes an executable portion. The method also includes receiving from a user at the requesting device transaction approval data, wherein the executable portion of the transaction program includes a first set of codes configured to encrypt the transaction approval data. There is also included encrypting the transaction approval data using the first set of codes. There is further included transmitting, using a transaction program, the encrypted transaction approval data to the server to complete the electronic transaction.

[**0015**] In yet another embodiment, the invention relates to a method for completing a transaction request pertaining to an electronic transaction conducted over an electronic network having a server and a requesting device. The method includes receiving from the server at the requesting device a transaction program, which includes an executable portion. There is also included searching, employing the executable portion, for a transaction approval device associated with the requesting terminal. If the transaction approval device is detected, the method further includes employing the transaction approval device to approve the transaction request. If the transaction approval device is not detected, the method also includes employing an input device associated with the requesting device to approve the transaction request. The method additionally includes transmitting, using the requesting device, an approved transaction request to the server to complete the electronic transaction. The approved transaction request signifies an approval of the transaction request by a user via at least one of the transaction approval device and the input device.

[**0016**] In an embodiment providing a further level of security, the private key is stored on the portable device, encrypted. The decryption key is stored outside of the device, at a trusted 3rd party location. When the user attempts to make a signature the software sends a request for the decryption key, along with the user's password or pass phrase keyed in at the keyboard of the PDA, smart phone, or cell phone, to a server belonging to the trusted 3rd party. This password is usually, but not always, different than the password stored in the PEAD. The server checks the password or pass phrase and, if it is correct sends the decryption key to the portable device, where it is used once and immediately discarded.

[**0017**] These and other advantages of the present invention will become apparent upon reading the following deteiled descriptions and studying the various figures of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[**0018**] To facilitate discussion, **FIG. 1** shows a prior art electronic transaction system, including an automated teller machine (ATM).

[**0019**] **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.

[**0020**] **FIG. 3A** shows, in one embodiment of the present invention, a simplified schematic of the PEAD of **FIG. 2**.

[**0021**] **FIG. 3B** shows, in one embodiment, the format of representative transaction approval data.

[**0022**] **FIG. 4** illustrates, in accordance with one embodiment of the present invention, a logic block schematic of the PEAD.

[**0023**] **FIG. 5A** represents, in accordance with one embodiment of the present invention, a high level hardware implementation of the PEAD.

[**0024**] **FIG. 5B** illustrates one implementation of a PEAD wherein the PEAD circuitries are implemented on an IC.

[**0025**] **FIG. 5C** represents an external view of the PEAD of **FIG. 5B** after being embedded in a card-like package.

[**0026**] **FIG. 6A** illustrates an external view of the PEAD in accordance with a preferred embodiment of the present invention.

[**0027**] **FIG. 6G** illustrates, in a simplified manner and in accordance with one aspect of the present invention, the hardware for implementing the PEAD of **FIG. 6A**.

Early Warning
IPR2024-01221
Ex. 1004-23

[0028] FIGS. 7A-B are flowcharts illustrating, in accordance with aspects of the present invention, the approval technique employing the inventive PEAD.

[0029] **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.

[0030] FIGS. 9A-B illustrate exemplary electronic transaction systems, including a transaction approval device, to facilitate discussion other aspects of the invention whereas a transaction program is employed to complete the electronic transaction.

[0031] **FIG. 10** illustrates an exemplary flowchart of a computer-implemented process which, in accordance with one embodiment of the present invention, permits a downloaded transaction program to complete an electronic transaction at the requesting device.

[0032] **FIG. 11** illustrates an exemplary transaction request to facilitate discussion.

[0033] FIGS. 12A-B illustrate an exemplary embodiment of the PEAD in accordance with an embodiment of the present invention.

[0034] **FIG. 13A** is a block diagram of an embodiment of this invention;

[0035] **FIG. 13B** is a flow chart of the operation of the embodiment of **FIG. 13A**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0036] FIGS. **2-12**B illustrate, 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, as described in the above referenced applications. **FIGS. 13A and 13B** illustrate a useful modification of these systems.

[0037] 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 checkout terminal, a portable device, hand-held device 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**.

[0038] 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 in this field.

[0039] 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 time 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**.

[0040] 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**.

[0041] 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.

[0042] 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 have 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.

[**0043**] 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/D13 Working Draft dated Nov. 12, 1999, available from IEEE Standards Dept. 345 East 47th Street, New York, N.Y. 10017-2349.

[**0044**] 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.

[**0045**] 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 passwords 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 read into the requesting device of the electronic transaction system, again exposing this data to interception or theft once read.

[**0046**] 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 the PEAD **200**. Since the identification data and/or the user's private key are never exposed, security risks to these data are substantially minimized.

[**0047**] **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.

[**0048**] 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 or audio output 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**.

[**0049**] 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.

[**0050**] 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 the 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.

[**0051**] 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 if 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. 3**B, 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.

[**0052**] 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 are 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.

[**0053**] **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**.

[**0054**] 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**.

[**0055**] 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**.

[**0056**] 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**.

[**0057**] Note that once the configuration data is decrypted and written into user identification 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 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).

[**0058**] 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.

[**0059**] If a greater level of security is desired, the user's private key may be optionally be scrambled or randomized prior to being written in to 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 the user's private key block **304**.

[**0060**] 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.

[**0061**] **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 microcontroller, discrete logic, programmable logic, an application-specific integrated circuit (ASCI), or the like, for implementing encryption logic **300** of **FIG. 2** and optionally decryption logic **402** of **FIG. 4**.

[**0062**] 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, electri-

Early Warning
IPR2024-01221
Ex. 1004-26

cally 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 the 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**.

[**0063**] 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 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 use.

[**0064**] 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.

[**0065**] 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 invented design.

[**0066**] 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.

[**0067**] In one embodiment, PEAD **200** may be implemented using a general purpose portable computing device, such as any of the miniaturized portable computers, personal digital assistants (PDA's) or portable phones that are currently popular. A PDA such as the Apple Newton or 3COM's Palm VII, for example, may be employed to implement PEAD **200**. Additionally, portable phones such as the Nokia 7110 Media Phone, Ericsson R280 SmartPhone or Motorola i1000 plus can be employed to implement the PEAD **200**. In this case, it is understood that the portable device such as a PDA, Media Phone or SmartPhone can be a requesting device itself, which communicates a remote electronic transaction system through a wireless network. The PEAD functionality can be embedded into such a portable requesting device. Such embodiments may usefully utilize a further level of security to be described below with respect to **FIGS. 13A and B**.

[**0068**] **FIG. 5B** illustrates one implementation of a PEAD wherein the circuitries are implemented on IC. In **FIG. 5**B, 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. 5**A, 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. 5**B, are also shown.

[**0069**] **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. 5**A, 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**.

[**0070**] **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 RESET the circuitry, including erasing the private key in the memory.

[**0071**] There is shown an infrared communication port **602** for receiving and transmitting data vis-à-vis the elec-

Early Warning
IPR2024-01221
Ex. 1004-27

tronic 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.

[**0072**] Optional display **610** may be implemented using any type of display technology such as liquid crystal technology. Display **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 or by audio output on the PEAD. Optional user authentication mechanism **612** prevents PEAD **200** from being used for approving transaction 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 fingerprints 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. The PEAD **200** can be built-in a portable phone such that port **602** can be a wireless communication and/or infrared port, display **610** can be a display on the portable phone, and buttons **606** and **608** are button keys on the portable phone key pad.

[**0073**] For example, user authentication mechanism **612** can be a Fingerchip FC15A140, a thermal silicon fingerprint sensor from Thomson-CSF of Totowa, N.J. Since no optics or light sources are needed as the finger's own heat produces all that is necessary to image the finger print, this implementation can be quite compact. In this embodiment, the user can authenticate himself/herself and approve a transaction through PEAD by simply presenting or sweeping his/her finger to/across the sensor **606**, thereby rendering approve button **606** optional. As another example, the mechanism **612** can be FPS **110**, a capacitive silicon finger print sensor from Veridicom of Santa Clara, Calif.

[**0074**] **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, Ill. such as the NC68HC05SC28, or security controller of SLE 22, 44 and 66 family from Infineon Technologies of San Jose, Calif. such as SLE66CX320S. 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.

[**0075**] **FIG. 7A** 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.

[**0076**] 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.

[**0077**] **FIG. 7B** is a flowchart illustrating, in accordance with another aspect of the present invention, the approval technique employing the inventive PEAD. In step **752**, a transaction request is received at the agent server from the requesting device associated with the electronic transaction system. In step **754**, the user has the option whether to approve or disapprove the transaction proposed at the PEAD. 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.

[**0078**] 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 **758**, which can occur either within the PEAD or the agent server or both. In step **760**, the encrypted transaction approval data is transmitted to the requesting device of the electronic transaction system after being encrypted.

[**0079**] **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. 3**B, 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.

[**0080**] 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.

[**0081**] 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.

[**0082**] 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. 6**A, 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.

[**0083**] 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 it is unlikely for a user to purchase multiple identical dinners at the same restaurant at a given time and date.

[**0084**] It should be noted that while the discussion above 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.

[**0085**] 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.

[**0086**] In another embodiment, the invention relates to techniques for conducting electronic transactions within an electronic transaction system such that confidentiality, authentication, integrity, and non-repudiation are substantially assured. It is observed that successful electronic transactions (e.g., those conducted over a computer network such as the Internet) have four major requirements: confidentiality, authentication, integrity and non-repudiation. In the prior art, confidentiality is typically addressed by employing encryption to encrypt data between the user's computer and the remote server. One such encryption technique employed by NetScape Corp. of Mountain View, Calif. involves the use of a Secure Socket Layer (SSL), which essentially utilizes encryption (e.g., public key encryption) for the point-to-point communication over an open network.

[**0087**] Although encryption techniques like SSL can, to a certain degree, ensure that the transmission of a transaction is secure, there is however no mechanism to authenticate the identity of the person who actually conducted the transaction (i.e., there is an authentication deficiency). By way of example, if an unauthorized person, after cracking a legitimate user's password, employs that legitimate user's computer (which may be SSL-enabled) to conduct a transaction to the detriment of the legitimate user, there is no mechanism to determine during or after the transaction is completed whether the person conducting the transaction in question is an unauthorized person or the legitimate user. Even if the legitimate user himself conducted the transaction, the authentication deficiency renders it impossible to guarantee non-repudiation, as it is difficult for the vendor to prove that it is indeed the legitimate user who conducted the transaction in question. Furthermore, although the transmission is relatively secure using a secured transmission facility such as SSL, the transmitted data (such as terms in a contract or purchase order) may be susceptible to being modified after it is decrypted by personnel at the receiving end.

[**0088**] In accordance with one aspect of the present invention, there is provided a software-implemented technique for performing electronic transactions in a manner such that the aforementioned requirements may be better addressed. In one embodiment, the electronic transaction technique proposed herein employs a transaction program (TP), which is essentially a program or an applet that may be downloaded into the requesting device (e.g., device **202**) from a server and executed at the requesting device to carry out the electronic transaction. By way of example, computer languages such as Javaä by Sun Microsystems Inc. of Mountain View, Calif. or ActiveX® by Microsoft Corp. of Redmond, Wash., or HDML (Handheld Device Markup Language) by Unwired Planet, Inc. of Redwood City, Calif. or WML (Wireless Markup Language) by Wireless Application Protocol Forum Ltd., may be employed although the electronic transaction technique proposed herein may be implemented by any other suitable computer language as well.

[**0089**] Once downloaded, the TP may be configured in any suitable manner for execution, preferably either as a stand-alone program or as a plug-in into one of the internet browsers (e.g., NetScapeä, Internet Exploreräor Microbrowser by the aforementioned NetScape Corp., Microsoft Corp. and Phone.com, Inc., respectively).

[**0090**] To facilitate discussion of the advantages and features of this aspect of the present invention, **FIG. 9A** depicts an electronic transaction network **900** including server **902**, network **904**, and requesting device **906**. A transaction

Early Warning
IPR2024-01221
Ex. 1004-29

approval device, such as PEAD **908** is also shown. Requesting device **906**, as mentioned earlier, may represent any device for permitting the user to transact business with the electronic transaction system. Preferably, the requesting device is implemented by a suitable computer terminal that is capable of communicating with server **902** through network **904**, which may represent a LAN, WAN, or the Internet. The computer terminal itself may be, for example, a desktop device, a portable device, a hand held device, or otherwise, including those implementing the Windows, Macintosh, Unix platforms or those capable of supporting a browser program. If the requesting device is a portable device, or hand-held device, then the PEAD **908** can be embedded into the requesting device **906**. Also, the communication link between the requesting device **906** and the server **902** can be a wireless communication link as shown in **FIG. 9B**.

[0091] To carry out an electronic transaction in accordance with one embodiment of this invention, the transaction program (TP) is preferably downloaded from the vendor's or service provider's server **902** into requesting device **906** (step **1002** of **FIG. 10**). The TP may include an executable portion as well as data related to the transactions for the user's input approval, and/or authentication.

[0092] By way of example, if the transaction involves the purchase of an appliance, the TP may download data pertaining to the model, price, and the like. **FIG. 11** depicts one exemplary transaction request for the purchase of appliances. As another example, if the transaction involves the purchase or sale of securities (such as stocks or bonds), the TP may be downloaded with data pertaining to the securities to be transacted. Of course, the transaction request may be related to any type of transaction, including those that do not involve the exchange of cash or credit for goods or services (such as document transfer).

[0093] In return, the TP preferably receives user's data from the user (e.g., the user's identification data, any data which may be required for the proposed transaction such as the address information, quantity information, size information, method of payment, credit card number, account number, and the like), and an indication of approval of the transaction.

[0094] It should be appreciated that the specific data to be downloaded may vary depending on the nature of the transaction to be performed. Likewise, the data to be received by the TP from the user may vary with applications. In some cases, if the user has already supplied the vendor with some of the requested data in the past (such as the user's address), the TP may not ask for the same data again or may simply present the already supplied data to the user for validation and/or possible editing.

[0095] The executable portion of the TP preferably includes codes to automatically detect the presence of a transaction approval device (such as the aforementioned PEAD), a smart card device, a Credit Card Reader, or the like) so that the TP can employ the transaction approval device to complete the transaction (step **1004** of **FIG. 10**). By way of example, the downloaded code may be configured to search the user's computer to detect whether a transaction approval device has been installed or to use the user's computer communication port(s) to query for the existence of a transaction approval device that may be external of the user's computer. If the PEAD is embedded in a portable requesting device, then the PEAD detection is performed in the portable requesting device.

[0096] The executable portion of the TP may also include codes to obtain, through an appropriate input device, the user's identification for authentication. By way of example, the TP may obtain the user's signature, the user's facial image, finger print, voice print, DNA coding sequence through a tissue sample, or other unique biometrics or other unique identifying data. The obtained user's identification facilitates non-repudiation, i.e., it facilitates identification of the identity of the person conducting the transaction so that fraud detection may be improved or deniability may be minimized. Of course some of the identification data may already exist in the PEAD and if such identification data is obtained from the PEAD, the obtained identification may indicate at least that the person performing the transaction on the requesting device also has access to the PEAD.

[0097] It should be appreciated, however, that some or all of the executable portion may not need to be downloaded every time and may be loaded once into the requesting device for subsequent use. Of course, the fact that the executable portion of the TP is downloadable, and preferably downloadable with a transaction to be approved, greatly simplifies the task of enabling electronic transactions even when the transaction approval device is updated (e.g., with new technologies), the communication protocol between the transaction approval device and the requesting device changes, or when a new transaction approval device is installed with the requesting device. In these cases, the TP containing the updated codes appropriate for the updated/new transaction device and/or protocol may be downloaded into the requesting device, either automatically with a transaction or upon request by the user, to enable electronic transactions.

[0098] For ease of discussion, assume that the requesting device (e.g., the user's computer) is PEAD-enabled. In this case, the TP may communicate with the PEAD, once it has detected the presence of such a device, to obtain approval data, authentication data and/or any other required user-supplied information in accordance with techniques discussed (step **1006** of **FIG. 10**). By way of example, the TP may employ the communication port in the requesting device for communication with the PEAD. As any of the required user authentication and user-supplied data may be stored in the PEAD, the user's approval, authentication and/or other user-supplied data may be encrypted by the PEAD and transmitted back to the requesting device wherein the TP may employ such data for responding to the transaction request, including transmitting some or all of the encrypted data received from the PEAD back to the server (step **1008** of **FIG. 10**).

[0099] As can be appreciated from the foregoing, the use of the PEAD in conjunction with the TP ensures that the electronic transaction is confidential since the encryption facilities in the PEAD and/or the TP renders the transmission secure. Further, the electronic transaction is more securely authenticated since the user can be authenticated using the identification data within the PEAD (e.g., the aforementioned unique biometrics or unique identifying data such as fingerprint, DNA coding sequence, voice print, or the like).

[0100] Likewise, if the requesting device is enabled with another transaction approval device such as a Smart Card

Early Warning
IPR2024-01221
Ex. 1004-30

reader or a credit card reader, the TP may then request that the user approve, authenticate, and/or supply the requested data using the transaction approval device present (e.g., by inserting the Smart Card or credit card or other similar apparatus into the transaction approval device present), either alone or in combination with other data entry techniques (e.g., clicking on choices present on the screen, typing, speech input, or the like) to complete the transaction data requested.

[0101] On the other hand, if the requesting device is not enabled with a transaction approval device, the user may still proceed with the transaction by authenticating, approving and/or supplying the requested data conventionally using any of the aforementioned data entry technique (step **1006** of **FIG. 10**). The TP will then preferably (but not necessarily) format and/or encrypt the entered data, using, e.g., a public key transcription system, to transmit the transaction data back to the server to complete the transaction (step **1008** of **FIG. 10**). In this manner, the TP will be backwardly compatible with requesting devices that may not be equipped with a transaction approval device.

[0102] Note that since the downloaded TP is, in the preferred embodiment, endowed with encryption facilities, i.e., the encryption codes is included in the downloaded codes in this embodiment, the presence of a general purpose encryption facility (such as the aforementioned SSL) may not be required for secured transmission. In this manner, backward compatibility with requesting devices which are not even equipped with a secured transmission facility (e.g., the aforementioned SSL) while transmission confidentiality is assured. On the other hand, if the requesting device is endowed with the general purpose encryption facility (e.g., the aforementioned SSL), the presence of the encryption codes in the TP may not be required. Of course, it is also possible to encrypt using both the encryption facility of the TP and the general purpose encryption facility (e.g., the aforementioned SSL) together to encrypt data transmitted to the server.

[0103] It should be noted, however, a transaction conducted in this manner may be less secure than that conducted with a transaction approval device such as the PEAD since the user's identity may not be authenticated, or verified, to the vendor. Because of this, there may be no guarantee of non-repudiation since a user can later deny having conducted the transaction in question. Along the same line, the data integrity may be less secure since the transaction data may be modified once received at the remote server.

[0104] Another implementation of the invention is directed toward a service reservation transaction. In this implementation, the PEAD can perform service reservation, transaction and service authorization all in the same device. For example, the PEAD can perform a hotel reservation through wireless network and Internet and complete the transaction by providing the credit information with electronic signature performed by the PEAD. Once the hotel acknowledges the transaction, the hotel can transmit the service information including room number direction to the hotel, etc. as well as the encrypted electronic room key through the Internet and wireless network to the PEAD. When the user arrives at the hotel, he does not need to wait on the line for check-in, but rather can go directly to the room and use the PEAD pre-stored hotel electronic key to open the room door. The PEAD user can also use the PEAD to order room service through the wireless network and Internet. At the end of the stay, the user can checkout through the PEAD and receive the electronic bill/receipt over the wireless network and Internet. For example, the user can check-out of the hotel while traveling to the airport to catch a flight.

[0105] Similarly, the PEAD can perform the airline ticket reservation through the wireless network and Internet. Once the transaction is completed using the PEAD, the airline can issue the encrypted electronic ticket through the Internet and wireless network to the PEAD. When the PEAD user arrives at the airport, after the security clearance, he can go directly aboard using the PEAD pre-stored electronic ticket to notify the gate counter computer that he is the ticket owner through the wireless network and Internet.

[0106] Similarly, the PEAD can be used to reserve theater tickets and receive the encrypted electronic tickets and service information through the wireless network and Internet. The PEAD can be used for rental car reservation, key pickup service, and even to start the car through an equipped Internet controlled ignition system, and car return service.

[0107] Or the Supermarket can issue electronic coupons through the Internet and wireless network to the PEAD. When the user shops in the Supermarket, he can present the coupons over the point of sale counter through the wireless network and Internet.

[0108] One of the preferred embodiments is using an Internet enabled cellular telephone (e.g., a web phone), a wireless PDA or a wireless two way pager to implement the PEAD to perform the above applications. The description below uses an Internet enabled cellular telephone as example of the implementation, and those skilled in the art will understand that the same or similar method can be applied to wireless PDAs and two way pagers. The Internet enabled cellular phone (web phone) can communicate with the Internet through a wireless network. For example, currently SprintPCS provides an Internet phone service using NeoPoint 1000 web phone. The web phone can access the Internet through a wireless gateway, and can contact the hotel's Internet reservation system through the wireless network and Internet. The software and/or firmware controls the PEAD functions running in the web phone is called eSignX Agent (or xAgent for short). xAgent is under the user's control to contact the hotel reservation transaction system. The reservation transaction process includes: (1) the web phone (PEAD) sending out the reservation request (optional using merchant public key [in the example given here, the merchant is the hotel, then it would be the hotel's public key or it's certificate] to encrypt the request; optionally using the user's private key to sign the request); (2) the Merchant acknowledges with the service availability and the cost (optionally, this message can be encrypted using the user's public key and the hotel's private key); (3) once the user approves the transaction, the web phone sends out the transaction confirmation with the credit information and signed by the user's private key (optionally encrypted with the Merchant's public key); (4) once the Merchant validates the transaction, the Merchant sends out the service information as well as the service authorization token (the token could be the electronic room key in the hotel reservation example, the token could be the electronic ticket in the

Early Warning
IPR2024-01221
Ex. 1004-31

Airline Ticket Reservation and Theater Ticket reservation examples, or the token could be the Supermarket coupon etc.). The token is optionally encrypted by the user's public key and Merchant's private key; (5) when the service is rendered, a service authorization token is to be presented over the point of service (example, hotel room door, airport boarding gate, or theatre entrance, Supermarket check-out counter or rental car etc.) through the wireless network and Internet; (6) if the service authorization token has been validated at the point of service (e.g., decrypting the token using the Merchant's public key successfully) then, the Merchant can authorize the service (e.g., to open the hotel room, to permit the boarding at the airport gate, to admit entering the theater, to discount the transaction amount, to ignite a car, etc.).

[0109] An implementation involving stock trading is performed in real time with the user by providing a buy or sell message for the user's approval. For example, a user may want to buy or sell stocks on a PEAD. Alternately, the user can set a limit to buy stock A at $50, and when the stock hits $50, the stock xAgent sends a push message to ask the user whether to buy or wait. The user can think about whether the stock will keep going down, and can enter a lower buy amount, say $48 and send back the confirmation to wait with an eSignX digital signature. The next time when the stock is at $48, a push message is again sent, but this time the user decides to buy and replies the pushed message with an eSignX digital signature to buy. Similarly the limit can be set as the percentage of the stock price, when the stock price rise about or fall below certain pre-determined or user defined percentage, the stock xAgent push a message to user for user's decision to buy or sell or wait with eSignX digital signature's approval. This technique can also be used for stock selling or other types of trades.

[0110] An implementation using a delivery service (e.g., FedEx or UPS) receipt signing can be achieved as well. For example, the PEAD can be used for getting FedEx and UPS to use a digital signature during delivery, especially when the recipient is not at the delivery location. One scenario is for example, Josh knows that he is getting a package today from FedEx, however when FedEx arrives, Josh is not around to receive it. FedEx pushes a message to a user's WAP phone asking whether the person can sign off for Josh and leave the package at the door (note the user or person could be Josh himself). Josh approves leaving the package at the door via eSignX for the transaction and FedEx leaves the package at door.

[0111] An implementation for mobile bidding includes the ability to view and enter bidding orders in real-time. Using PEAD (e.g., mobile phone), the user can bid on the phone. Bidding house like eBay required users to bid on a computer and to be constantly monitor the auction to avoid losing the item. This is frustrating to many users and the eSignX service presents a solution by allowing the user to select notification of out-bid and action to ignore and forego, or to raise bid. The push message is sent when the ignore or raise bid action is required.

[0112] One of the preferred embodiments for the above three implementations (stock trading, delivery sign off and mobile online bidding) is using an Internet enabled cellular telephone (e.g., a web phone), a wireless PDA or a wireless two way pager to implement the PEAD to perform the above applications. The description below uses an Internet enabled cellular telephone as an example of the implementation, and those skilled in the art will understand that the same or similar method can be applied to wireless PDAs and two-way pagers. The Internet enabled cellular phone (web phone) can communicate with the Internet through a wireless network. For example, currently SprintPCS and GTE provide an Internet phone service using NeoPoint, StarTAC web phone, etc. The stock trading system, delivery sign-off system or the mobile online bidding system through the wireless network and Internet can push the confirmation message to the web phone for approval. The user can digitally sign the transaction message using the user's private key by the PEAD embedded in the web phone to confirm the transaction. Or the user can modify the transaction message and digitally sign the modified transaction message using the PEAD embedded in the web phone. For example, in the stock trading system, when a stock exceeds predetermined price fluctuation (up or down say 10%), the system will push a message to the user's web phone over the Internet and wireless network and request for action, say to sell. The user can modify the transaction message to hold or adjust the fluctuation threshold to higher percentage and then sign the modified transaction message and send it back to the stock trading system through wireless network and Internet. Similarly for the delivery sign-off system, upon user receiving the confirmation message, the user can modify the next delivery time slot or accept the package at the different place. For the mobile online bidding system, upon user's offer being out bid by others, the system push a message to the user's web phone for action item either withdraw, or offer a new bidding price. All the above modified confirmation or bidding price need to be digitally signed using the user's private key by the PEAD embedded in the web phone.

[0113] In yet another implementation, called a Point-of-Sale Transaction, the PEAD can perform the Point-of-Sale Transaction through the wireless network and Internet. In the future, the Point-of-Sale terminal can access the Internet through an internal network system or through a dial-up phone line, DSL, ADSL, or cable modem, etc. FIGS. **12**A-B show an exemplary PEAD that can be used as the Point-of-Sale Transaction device including a scanner **1602**. At the Point-of-Sale check-out counter, the Point-of-Sale terminal can scan in the merchandise barcodes and generate transaction information as well as generate a unique transaction number (which contains the store number+counter number+transaction number for example) or a unique ID of the Point-of-Sale terminal (e.g., a phone number) to give to the PEAD user to enter into the PEAD (for example the web phone). The user can use the keypad on the PEAD to enter the unique ID of the Point-of-Sale terminal or use an alternative input device built into the PEAD such as a barcode scanner or OCR reader to scan in the unique ID of the Point-of-Sale terminal. It is also possible to enter the merchandise bar code number to the PEAD through the keypad or scanner on the PEAD and generate transaction information from the PEAD rather than generate the transaction information from the Point-of-Sale terminal. Then the PEAD can use this unique transaction number or a unique ID of the Point-of-Sale terminal to establish the communication link with the Point-of-Sale system through the wireless network and Internet to conduct the transaction. Or, the user can give the Point-of-Sale counter the unique PEAD ID

Early Warning
IPR2024-01221
Ex. 1004-32

(e.g., a cellular phone number) to enter into the Point-of-Sale terminal or the Merchant can use the scanner (e.g., barcode scanner or OCR scanner) to scan in the PEAD ID that is attached on the external case of the PEAD in barcode and/or human readable format to establish the communication link with the PEAD through the Internet and wireless network to conduct the transaction. This identification process (or link-up process) can be automated through local wireless port for example: the infrared port or a Bluetooth (short range wireless RF) port. Alternately, the PEAD can be equipped with a GPS system, then the PEAD can search automatically the closest Point-of-Sale terminal according to GPS geometry position and establish the link automatically by using a Location-ID mapping table that maps the proximity of the Point-of-Sale terminal location to the unique ID of the Point-of-Sale terminal. Once the link between the PEAD and Point-of-Sale terminal is established, the PEAD can display the transaction information including the price, items, etc., and if the user agrees to pay, he will press the approve button to authorize the transaction. The user approval process and transaction process using the PEAD is also described in U.S. Ser. No. 09/067,176 and U.S. Ser. No. 08/759,555, now U.S. Pat. No. 5,917,913.

[0114] In an aspect of the invention, if the Point-of-Sale terminal also has short range wireless communication capability such as Bluetooth and infrared communication port, the described transaction can be conducted locally through PEAD's Bluetooth port or infrared port using the same method.

[0115] Another implementation of Point-of-Sale Transaction is to use PEAD as self checkout terminal. By entering the UPC code or barcode using keypad on the PEAD or scanning in the UPC code or barcode using the input device built into the PEAD such as a barcode scanner or OCR reader, the PEAD can generate the receipt with the list of item prices through the wireless network and Internet by querying the item price using the barcode as the index for price lookup table which is stored in a server system. The PEAD user can sign the receipt electronically using PEAD as described in U.S. Pat. No. 5,917,913. One of the preferred embodiments of the PEAD self checkout terminal is to use a PEAD embedded cellular phone such as a WAP enabled phone (WAP phone) with WIM as specified in the WAP 1.2 standard published by the Wireless Application Protocol Forum Ltd. A scanner module can be plugged into the WAP phone I/O port to function as an standard input device. Or a scanner module can be built into the cellular phone and function as an standard input device. It is understood that an infrared port and Bluetooth port can be both of the standard I/O ports built-in into the cellular phone for short range wireless communication. For example, when a WAP phone user goes to a store, the user can enter the StoreID to activate the checkout functionality and to connect to the store price table database through wireless network and/or Internet. (It is understood that this connection can be done automatically when the GPS or the equivalent system is used to locate the user position and then translate the StoreID automatically through the table lookup database as described in the previous section. Or use the barcode scanner of the cellular phone to scan in the StoreID posted in the store. Or through the Bluetooth short range radio to broadcast the StoreID in the store premises.) Then the user only needs to scan in (or key in) the barcode of the product she/he would like to purchase in the store. The cellular phone would display the price of the item the user entered (or scanned in). If the user agrees to pay for the item, the user can approve the transaction by pressing the button on the phone. The approval process using the PEAD is described in U.S. Pat. No. 5,917,913. The user can then walk out the store by presenting the electronic receipt over the phone or goes to the receipt printer to print out the hardcopy. The method of establishing connection between cellular phone and printer to print out the hardcopy receipt is either to enter the cellular phone number (subscriber ID) into the printer or use the phone scanner to scan in the receipt printer ID or just enter the receipt printer ID into the cellular phone and request to print out the receipt hardcopy. The alternative method of establishing the connection between the cellular phone and the receipt printer is through local wireless communication port such as infrared and short range RF to exchange the printer ID and/or the user subscriber ID such as the cellular phone number. The receipt printer is connected to the Intranet/Internet and can access the user's receipt data through xAgent or xMerchant server then to print out the receipt.

[0116] Additionally, a Universal Point-of-Sale Application can be achieved. Using PEAD Self Checkout Terminal such as the WAP phone to order merchandise through wireless network and Internet, the WAP phone users can buy merchandise wherever and whenever they see the products, and may not necessary in the store. They might see a product in their friend's home and enter or scan in the product ID or UPC code or barcode into the PEAD. The xAgent running in the PEAD or in a remote Agent server will place the order automatically for the PEAD users. Then the products will be delivered to the user, or the user can pick up the order at specified store at certain schedule. The order can be either placed immediately or accumulatively until certain criteria are met, for example, when total order exceeds $100, or orders are accumulated by the end of the week, or until a bargaining price set by the user is found. When an order is confirmed, the user needs to sign an order electronically through PEAD as described in U.S. Pat. No. 5,917,913.

[0117] It is understood that the PEAD self checkout terminal may not necessary is implemented as WAP enabled phone; it can be implemented by any web enabled cellular phone and may not necessary using WAP protocol.

[0118] It is also possible to use an ordinary cellular phone not necessarily having web capability to perform both above Service Reservation Transaction and Point-of-Sale Transaction by using a remote voice activated or touch tone server. For example, this is called an Agent Server. The Agent Server functions exactly like the PEAD in a web phone except it is not necessarily portable. It operates through the existing voice activated or touch tone interfacing with the end user through the existing phone network. Once the user registers an xAgent in the Agent Server, the ordinary cellular phone end user can enjoy all the same functionality as the web phone user. For example, the end user can use the ordinary cellular phone to dial in to the Agent Server to activate his own xAgent by entering his xAgent password through voice activated interface or touch tone interface. Once xAgent is activated, it can reserve a hotel room, order tickets, pay at a point-of-sale counter through the Agent Server, just as if it were running on a web phone. For example, the end user can reserve a hotel room, once the xAgent gets approval from the user's cellular phone, the

Early Warning
IPR2024-01221
Ex. 1004-33

xAgent running on the Agent Server can exchange the credit information pre-stored in the xAgent and sign the transaction. The hotel can issue the electronic room key to the xAgent in the Agent Server just the same as to the PEAD. When the end user arrives at the hotel, he can dial the Agent Server number to request to activate the electronic room key stored in the xAgent to open the door through the Internet. Similarly, all other applications that can be conducted through a web phone, can also be conducted by the ordinary cellular phone plus the remote running xAgent in the Agent Server.

[0119] In a wireless PDA, SmartPhone, or a cellular phone, in some circumstances there may not be a special tamper proof hardware such as SIM (Subscriber Identity Module) or WIM (Wireless Identity Module) for the storage of the private key. In this case, to protect the private key, an encryption key of sufficient strength must be used. That encryption key must be protected against compromise.

[0120] In designing a solution to this problem, one must assume that a potential attacker has access to all of the memory within the device, and has a complete understanding of the functioning of the encryption software. Assuming these two things, an optimum way to protect the private key is to encrypt it with strong encryption, as described above. In addition, the encryption key for that strong encryption can be stored somewhere other than in the device. If this key were to be stored on the device itself, an attacker with an understanding of the software could find that key, regardless of how well the system manages to "obscure" it.

[0121] The solution, as illustrated in **FIG. 13**A, is to add to the system described above, for example, with respect to **FIG. 2, a** third party server **1302** to be used to implement an added level of security. In this approach, where a cell phone, PDA, or the like **1310** serves as or otherwise incorporates the functions of the PEAD **200**, the private key is stored on the portable device, encrypted. The decryption key is stored outside of the device, at a trusted 3rd party location. When the user attempts to make a signature, as shown in the flow chart of **FIG. 13**B, the software sends **1350** a request for the decryption key, along with the user's password or pass phrase keyed in at the keyboard **1312** of the PDA, smart phone, or cell phone, to a server **1302** belonging to the trusted 3rd party. This password is usually, but not always, different than the password stored in PEAD **200**. The server checks **1352** the password or pass phrase and, if it is correct **1354** sends the decryption key to the portable device, where it is used once and immediately discarded. It is understood that the secure communication link such as SSL or WTLS is used while transmitting the user's password or pass phrase as well as the decryption key to prevent eavesdropping.

[0122] If the password or pass phrase provided to the server is incorrect, the event is recorded and the portable device is informed **1356**. Once a certain number of failures have occurred (three or five, mostly likely), the server or PEAD will deactivate **1360** the account and refuse to provide the decryption key, even if further attempts supply the correct password or pass phrase. This ensures that an attacker is only permitted three or five attempts to violate the integrity of the system, before they must resort to an unfeasible brute-force attack against the encryption itself.

[0123] A preferred method can be used to protect the private key stored in the regular non-volatile memory in the portable device from the above stated attack. The method is to encrypt the private key with an efficient symmetric key scheme such as 3DES and store the encrypted private key in the memory. The 3DES key is then stored in a remote server **1302** corresponding with an authorization password or pass phrase. Whenever the user needs to digitally sign a transaction, the portable device will request the user to key in the password or pass phrase and send it to the remote server to request the 3DES key. Once the remote server verifies that the password or pass phrase is valid, then it sends back the 3DES key to the portable device for decrypting the private key for signing the transaction. It is understood that the secure communication link such as SSL (Secure Socket Layer) or WTLS (Wireless Transport Layer Security) is used for transmitting the user's password or pass phrase as well as the 3DES key. After finishing the signing process, both 3DES key and plain private key will be deleted from the RAM. In this method, the password or pass phrase are not stored in the portable device; only the encrypted private key is stored in the portable device. Furthermore, the remote server will monitor any unauthorized access of the 3DES key, for example, after three or more trials of an incorrect password or pass phrase, the server will automatically disable further access to the 3DES key and immediately notify the PEAD user through e-mail alert, phone call, or short message alert, etc. It should be understood that the above method can also be used in an electronic authorization system such as PC or Workstation connected to the electronic transaction system through wireless network and/or Internet.

[0124] The many features and advantages of the present invention are apparent from the written description, and thus, it is intended by the appended claims to cover all such features and advantages of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

What is claimed is:

1. In a portable electronic authorization device (PEAD) without tamper proof storage of a user's private key, a method for approving a transaction request originates from an electronic transaction system, comprising:

receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request; and

if said transaction request is approved by a user of said portable electronic authorization device, decrypting the user private key using a decryption key from a remote server, and transmitting a second digital data to said electronic transaction system, said second digital data being encrypted by said user private key.

2. In an electronic authorization system without tamper proof storage of a user's private key, a method for approving a transaction request originating from an electronic transaction system, comprising:

receiving at said electronic authorization system first digital data, said first digital data representing said transaction request; and

Early Warning
IPR2024-01221
Ex. 1004-34

if said transaction request is approved by a user of said electronic authorization system, decrypting the user private key using a decryption key from a remote server, transmitting a second digital data to said electronic transaction system, said second digital data being encrypted by said user private key.

3. A method as claimed in claim 1 wherein decrypting the user private key includes sending a request from the PEAD to the server including a password from the user of the PEAD.

4. A method as claimed in claim 3 wherein the request includes transmitting a user password or pass phrase.

5. A method as claimed in claim 4 wherein the password or pass phrase is keyed in at the PEAD.

6. A method as claimed in claim 5 wherein if the password or pass phrase provided to the server is incorrect, the PEAD is informed and the event is recorded.

7. A method as claimed in claim 6 wherein once a certain number of failures due to an uncorrected password or pass phrase have occurred, the users account associated with the private key is deactivated.

8. A method as claimed in claim 7 wherein upon deactivation of the account, the server will refuse to provide the decryption key.

9. A method as claimed in claim 1 wherein the user private key is stored in the PEAD encrypted with a symmetric key scheme.

10. A method as claimed in claim 9 wherein the symmetric key scheme is 3DES.

11. A method as claimed in claim 10 wherein the 3DES key is stored in the remote server associated with an authorization test password or pass phrase for the user.

12. A method as claimed in claim 11 wherein whenever the user needs to authorize a transaction, the user inputs the password or pass phrase at a keyboard at the PEAD.

13. A method as claimed in claim 12 where upon the password or pass phrase being keyed into the PEAD, it is transmitted to the remote server, the remote server returning the symmetric key to the PEAD for decrypting the private key.

14. A method as claimed in claim 13 wherein after finishing the signing process, both the 3DES key and the plain private key, the password or pass phrase entered by the user are deleted from the PEAD.

15. A method as claimed in claim 14 wherein the remote server will monitor and detect any unauthorized attempted access of the symmetric key stored at the server, and notifies the PEAD user through e-mail alert, phone call or message alert.

16. A method as claimed in claim 2 wherein decrypting the user private key includes sending a request from the electronic authorization system to the server including a password from the user of the electronic authorization system.

17. A method as claimed in claim 16 wherein the request includes transmitting a user password or pass phrase.

18. A method as claimed in claim 17 wherein the password or pass phrase is keyed in at the electronic authorization system.

19. A method as claimed in claim 18 wherein if the password or pass phrase provided to the server is incorrect, the electronic authorization system is informed and the event is recorded.

20. A method as claimed in claim 19 wherein once a certain number of failures due to an uncorrected password or pass phrase have occurred, the users account associated with the private key is deactivated.

21. A method as claimed in claim 20 wherein upon deactivation of the account, the server will refuse to provide the decryption key.

22. A method as claimed in claim 2 wherein the user private key is stored in the electronic authorization system encrypted with a symmetric key scheme.

23. A method as claimed in claim 22 wherein the symmetric key scheme is 3DES.

24. A method as claimed in claim 23 wherein the 3DES key is stored in the remote server associated with an authorization test password or pass phrase for the user.

25. A method as claimed in claim 24 wherein whenever the user needs to authorize a transaction, the user inputs the password or pass phrase at a keyboard at the electronic authorization system.

26. A method as claimed in claim 25 where upon the password or pass phrase being keyed into the electronic authorization system, it is transmitted to the remote server, the remote server returning the symmetric key to the electronic authorization system for decrypting the private key.

27. A method as claimed in claim 26 wherein after finishing the signing process, both the 3DES key and the plain private key, the password or pass phrase entered by the user are deleted from the electronic authorization system.

28. A method as claimed in claim 27 wherein the remote server will monitor and detect any unauthorized attempted access of the symmetric key stored at the server, and notifies the electronic authorization system user through e-mail alert, phone call or message alert.

* * * * *

Early Warning
IPR2024-01221
Ex. 1004-35