(12) INNOVATION PATENT (11) Application No. **AU 2005100466 A4**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Embedded synchronous random disposable code identification method and system

(51)[7] International Patent Classification(s)
G07F 007/00

(21) Application No: **2005100466** (22) Date of Filing: **2005.06.02**

(45) Publication Date: **2005.07.07**
(45) Publication Journal Date: **2005.07.07**
(45) Granted Journal Date: **2005.07.07**

(62) Divisional of:
2003200600

(71) Applicant(s)
Swivel Secure Limited

(72) Inventor(s)
Keech, Winston Donald

(74) Agent / Attorney
Eagar & Buck, 21/36 Agnes Street, Fortitude Valley, QLD, 4006

ABSTRACT

A method and system for secure identification of a person in an electronic communications environment, wherein a host computer is adapted to be able to communicate with a specific electronic communications device operated by the person. The person is issued with a mask code, e.g. a PIN, known only to the person and stored in the host computer, but never transmitted electronically therebetween. When the person is required to identify him- or herself to the host computer, the host computer transmits a pseudo-random string to the specific electronic communications device, whereupon the PIN must be applied to the pseudo-random string according to predetermined rules so as to generate a volatile identification code which is then transmitted back to the host computer. In one embodiment positive identification is achieved when the volatile identification code matches a volatile identification code generated within the host computer by applying the mask code stored therein to the pseudo-random string. In this way, a person's mask code is never transmitted electronically and is therefore relatively safe from interception, and the volatile identification code will be different for each different pseudo-random string, thus making a fraudulently intercepted communication meaningless.

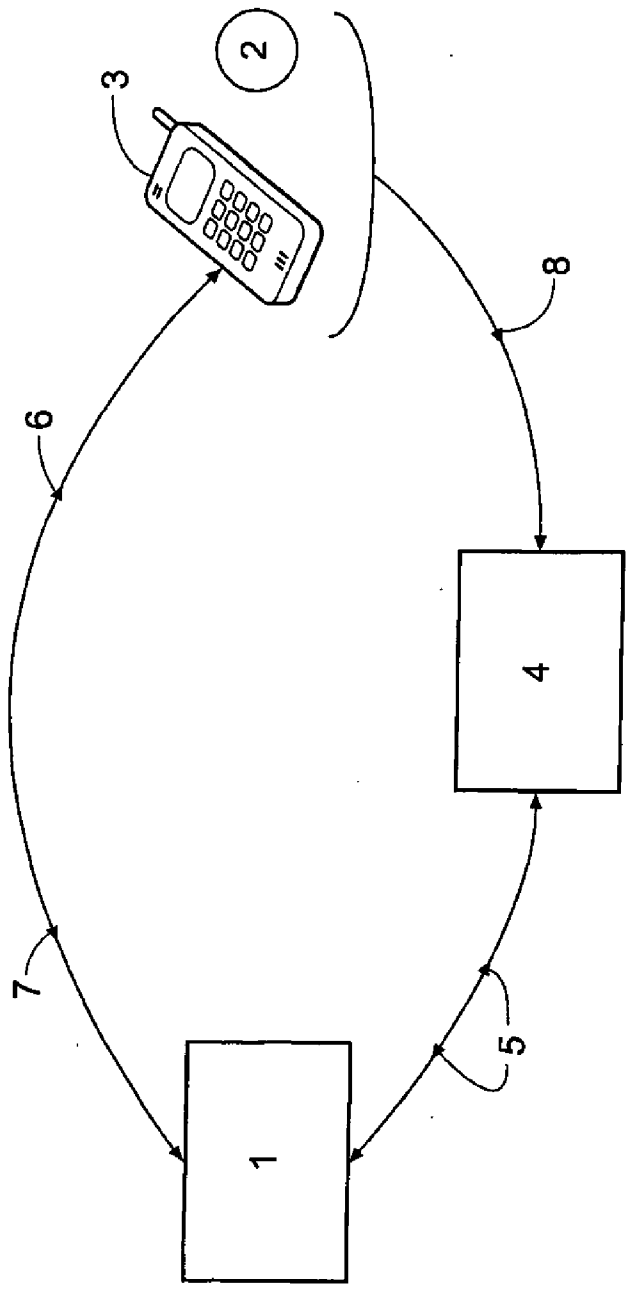

Fig. 1

AUSTRALIA

Patents Act 1990

COMPLETE SPECIFICATION

INNOVATION PATENT

EMBEDDED SYNCHRONOUS RANDOM DISPOSABLE CODE IDENTIFICATION METHOD AND SYSTEM

The following statement is a full description of this invention including the best method of performing it known to me

EMBEDDED SYNCHRONOUS RANDOM DISPOSABLE CODE IDENTIFICATION METHOD AND SYSTEM

The present invention relates to a system and method for identifying a user or device and, optionally, for conducting transactions between the user or device and a third party, for example by way of a telephone connection or an electronic computer system such as the Internet.

Various systems are known for conducting electronic transactions in a more or less secure manner over a telecommunications link or the like. One well known system is known as electronic funds transfer at point-of-sale (EFTPOS), in which a user is issued with a credit or debit card bearing a unique identification number, usually embossed on the card in human-readable form and also encoded on a machine-readable magnetic strip on the reverse of the card. For further identification purposes, the card typically includes space for a user permanently to include his or her signature. In use, when a user wishes to make a purchase in, for example, a retail store, he or she presents the debit or credit card to a store employee. The card is then swiped through a card reader, and information relating to the identity of the card, the identity of the retail store and the value of the goods or services being purchased is transmitted by way of a telephone connection to a remote computer server operated by the card issuer (normally a bank or suchlike). The remote computer server checks that the user's card account contains sufficient funds or credit to cover the proposed transaction, checks that the user's card account is currently operational (for example, to check that the card has not been reported stolen), and then issues a confirmation signal back to the card reader to indicate that the transaction may be authorised. The store employee must then obtain a specimen of the user's signature and compare this with the signature on the reverse of the card so as to check the identity of the user. If the signatures appear to match, the store employee operates the card reader to complete the transaction, and the funds required to cover the transaction are then electronically transferred from the user's card account to the retail store. If the signatures do not appear to match, then the store employee may request additional

proof of identification before authorising the transaction, or may simply refuse the transaction and retain the user's card, which may have been stolen, thereby preventing any unauthorised transfer of funds. This system is open to fraudulent abuse, since it is possible for a card to be stolen and for a thief to forge the signature of an authorised user.

In a development of this system, a card user may be issued with a personal identification number (PIN), which is usually a four digit code, and which is theoretically known only to the user and to the card issuer. Instead of or in addition to providing a specimen of his or her signature at the point-of-sale, the card user is required to enter his or her PIN into the card reader, and this information is transmitted to the remote computer server together with the card and retail store identification data and data regarding the value of the transaction. By providing an extra identification check by way of the PIN, this system helps to prevent fraud by forgery of signatures, but is still not completely secure because the PIN does not change between transactions, and may therefore be intercepted together with card identification data when being transmitted between the card reader and the remote server. Furthermore, it is possible for a thief to observe a user entering his or her PIN into a card reader and to remember the PIN. If the thief is also able to obtain card identification details, for example from a discarded till receipt or through conspiracy with the store employee, it is a simple matter to produce a fake card including all the appropriate identification information for later fraudulent use, or even to rob the authorised card user of his or her card.

Summary of the Invention

According to a first aspect of the present invention there is provided a method for verifying the identity of a user having a personal identification number (PIN), the method including the steps of:

2005100466 02 Jun 2005

i) forming display characters on a display of a computational device, the display characters being in correspondence with characters comprising the PIN to assist the user to input a volatile identification code derived from said PIN; and

ii) verifying the identity of the user on the basis of the volatile identification code.

According to a further aspect of the present invention there is provided a method for verifying the identity of a user, wherein the user has a personal identification number (PIN) comprising a first array of numbers, each number having a given numerical position in the first array, the method including the steps of:

i) forming a second array of display characters on a display of a computational device, each display character having a given numerical position in the second array;

ii) processing a volatile identification code input by the user upon application of the PIN to the second array; and

iii) verifying the identity of the user by checking that the volatile identification code matches a third array of characters formed by sequentially selecting display characters at numerical positions in the second array on the basis of the numbers in the first array, taken in positional order.

In one embodiment the display characters comprise letters of the alphabet.

Preferably the method is implemented by means of a network server programmed to implement a method as described above.

According to a further aspect of the present invention there is provided a software product bearing instructions for a computational device to implement the method.

Brief Description of the Figures

For a better understanding of the present invention and to show how it may be carried into effect, reference shall now be made, by way of example, to the accompanying drawings in which:

FIGURE 1 is a schematic diagram showing a preferred embodiment of the present invention;

FIGURE 2 is a schematic diagram showing a preferred embodiment of the dual channel schema;

FIGURE 3 is a process flow diagram showing the steps a user would take while interacting with the system of the present invention;

FIGURE 4 is a schematic diagram showing a preferred embodiment of the single channel schema of the present invention;

FIGURE 5 is a schematic diagram showing an additional embodiment of the single channel schema of the present invention;

FIGURE 6 is a schematic diagram of an additional embodiment of the single channel schema of the present invention;

FIGURE 7 is a schematic diagram of an additional embodiment of the single channel schema of the present invention;

FIGURE 8 is a schematic diagram showing an additional embodiment incorporating various aspects and features of the present invention;

FIGURE 9 is a schematic diagram showing a secured database access system of the present invention;

FIGURE 10 is a schematic diagram of a secure system for retrieving bank account information;

FIGURE 11 is a representation of pseudo-random string;

FIGURE 12 is a schematic diagram showing the modification and integration process of the user's temporary or transactional;

FIGURE 13a is a graphical representation of the user interface of the present invention;

FIGURE 13b is a graphical representation of the user interface of the present invention;

FIGURE 13c is a graphical representation of the user interface of the present invention;

FIGURE 13d is a graphical representation of the user interface of the present invention;

FIGURE 13e is a graphical representation of the user interface of the present invention;

FIGURE 13f is a graphical representation of the user interface of the present invention;

FIGURE 13g is a graphical representation of the user interface of the present invention;

FIGURE 13h is a graphical representation of the user interface of the present invention;

FIGURE 14 is a graphical representation of the start screen of the PIN Safe interface of the present invention;

FIGURE 15a is a graphical representation of the first cycle of the PIN Safe user interface;

FIGURE 15b is a graphical representation of the second cycle of the PIN Safe user interface;

FIGURE 15c is a graphical representation of the third cycle of the PIN Safe user interface;

FIGURE 15d is a graphical representation of the fourth cycle of the PIN Safe user interface;

FIGURE 15e is a graphical representation of the PIN Safe user interface using symbols or characters instead of numbers;

FIGURE 16 is a schematic diagram showing features of the present invention utilized in a database access system via the Internet;

FIGURE 17 is a schematic diagram containing features of the present invention utilized in the access of multiple databases via the Internet;

FIGURE 18 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet;

FIGURE 19 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet;

FIGURE 20 is a schematic diagram of various features and components of the present invention communicating via the Internet;

FIGURE 21 is a schematic diagram illustrating the access and data channels of an additional embodiment of the present invention;

FIGURE 22 represents a schematic diagram displaying a generic server gateway schema incorporating various aspects of the present invention; and

FIGURE 23 shows a schematic diagram illustrating a generic integration platform of the present invention.

Figure 1 shows a host computer 1 operated by a credit/debit card issuer, a user 2 having a mobile telephone 3, and an EFTPOS terminal 4. The user 2 is issued with a card (not shown) having a unique 16-digit account number embossed and magnetically encoded thereon, this 16-digit account number being correlated in the host computer 1 with account details relating to the user as well as a 4-digit mask code selected by or assigned to the user 2 upon initial registration with the credit/debit card issuer and a unique telephone number of the mobile telephone 3. The 16-digit account number is chosen for compatibility with existing credit/debit card protocols, and the 4-digit mask code for compatibility with existing PIN protocols. When the user 2 wishes to make a purchase from a retailer (not shown) operating the EFTPOS terminal 4, he or she presents the card, which is then scanned by the EFTPOS terminal 4. Details regarding a purchase are also entered into the EFTPOS terminal 4 by the retailer, and these are transmitted, together with the account number, to the host computer 1 by way of a modem link 5. The host computer 1 then correlates the account number with details of the user 2, including the telephone number of the mobile telephone 3, and generates a 13-digit pseudo-

random string which is transmitted to the mobile telephone 3 by way of an SMS or voicemail protocol 6. The first three digits of the pseudo-random string are not random and are reserved to indicate to the user that a received SMS message is from the host computer. For example, the first three digits may be "T1:" or "T2:" or the like, so as to indicate that the host computer 1 is expecting the user 2 to apply a first or a second mask code to the pseudo-random string. The next 10 digits of the pseudo-random string provide sufficient redundancy for any 4-digit mask code to operate thereupon in the manner hereinbefore described. By choosing a string length of 13 digits for the pseudo-random string, compatibility with existing mobile telephone displays and EAN13 (European Article Number) barcode protocols is ensured.

Upon reception of the pseudo-random string by the mobile telephone 3, the user 2 must apply the mask code thereto as hereinbefore described so as to generate a volatile identification code, which is then passed 8 to the retailer and entered into the EFTPOS terminal 4 for transmission to the host computer 1. Alternatively, the volatile identification code may be returned by the user 2 to the host computer 1 by way of the mobile telephone 3.

When the host computer 1 receives the volatile identification code, it compares this with a volatile identification code generated within the host computer 1 by applying the mask code to the pseudo-random string and, if the volatile identification codes are found to match, issues a signal to the EFTPOS terminal 4 so as to authorise the purchase and to transfer necessary funds to the retailer. Those skilled in the art will realise that other approaches to verifying the identity of the user on the basis of the volatile identification code may be taken. For example, host computer 1 may apply the received volatile identification code to the pseudo-random string that was issued to derive a test mask code. If the test mask code and the user's mask code are found to match the host computer then issues a signal to the EFTPOS terminal 4 so as to authorise the purchase.

Optionally, before authorising the transfer of funds, the host computer 1 may send a message to the mobile telephone 3, for example in SMS or voicemail format 6, preferably including details of the transaction, and requesting that the user 2 return a signal 7 so as finally to confirm the transaction. This may provide added peace-of-mind for unusually large transactions and may alert a user 2 in the event that fraudulent use is being made of his or her card.

The present invention may be implemented in both a single and dual channel schema which are disclosed and discussed in relation to Figures 2-10.

The Dual Channel protocol is appropriate for all users who own a G2 mobile phone. The types of transaction might include: (1) Electronic Funds Transfer at the Point of Sale (EFT/POS) and (2) Telephone orders. EFT/POS are transactions where the user would make a purchase at a merchant in the normal way and when the credit/debit card is swiped through the card reader, the merchant would be prompted to ask for the customer's transaction affirmation code (TAC) or mask code. The user remembers his or her four digit PIN number which is used to determine the TAC from the pseudo-random string, which is given at the point of sale. If the user intends to make multiple purchases within a short space of time or in an area where mobile phone reception is poor the user can elect in advance to use the same TAC for a single day. A telephone order transaction would essentially use the same method as above with the exception that the merchant physically enters the card details in the usual manner before being prompted for the TAC.

Additional features of the dual channel schema are that the customer will be able to choose alternative user-friendly methods of identifying the TAC from the pseudo-random security string. such as an Enigma interface or voice recognition system. An Enigma Interface would include minor modifications to a SIM card in a phone or pager during manufacture but customers could avoid any calculation of the TAC themselves. Users will be able to key in their PIN and by pressing an additional key of their choice, the phone or pager will automatically compute the resultant TAC,

without the customer even seeing the Security String. This computation would be a completely internal, ensuring that only the TAC is displayed, and the PIN is not retained in the mobile phone or pager. A voice recognition interface could be implemented in voice activated phones and be able to compute the appropriate TAC on the simple command "TAC!" from an approved voice.

Customers could also have the option of choosing, when applying for an enabled card, a geometric shape, as will be discussed in more detail below, in which the security string will always be delivered. The customer would simply register his or her chosen geometric shape to be displayed on screen and then visually apply his or her PIN pattern to determine the corresponding resultant TAC. This display can be interfaced by a WAP mobile phone, a G3 mobile phone, an Internet site display prompt or a secondary dedicated terminal placed at the point of sale.

The protocol of the present invention may be 'bolted-on' to an existing database server and can at least run on unmodified EFT/POS hardware such as: (1) AMEX ; (2) Split dial EPOS; and (3) VISA AVS3. In addition, the dual channel protocol can be used to upgrade the security of Mondex systems (these already use a 4-PIN digit at POS).

The dual demand schema may use a standard G2 mobile phone, G3, and WAP device to receive the security string. If these devices include a modified SIM card interface for this security string the device may also include a GUI or an Enigma interface to simplify the derivation of the TAC.

Figure 2 represents a diagram showing the protocol for the present invention applied to a point of sale environment. Figure 2 displays the main components and steps for this transaction and displays two different options. The first option utilizes a split dial electronic funds transfer point of sale machine (EFT/POS), where the details of the transaction are directly sent via the Authorization Server 207. The second option utilizes the merchant acquirer's network.

In the direct dial scenario, the user 201 receives a security string 210 from the Authorization Server 207 which resides on the device 202. The security string 210 resides on the device 202, such as a mobile phone, until the user is ready to make a purchase. When the user 201 is ready to make a purchase he or she hands over, in step 220, his or her enabled credit card 204 to a merchant 205 to conduct the electronic funds transfer or point of sale (EFT/POS). The card 204 is swiped as usual at the merchant's 205 EFT/POS terminal. The user 201 reviews the security string 210 residing on his or her device 202 and determines his or her TAC for that particular sale. The four digit TAC 230 is provided to the merchant 205 by the user 201. The user 201 may provide the TAC verbally, by entering it into the POS terminal, or by entering the number on the mobile device 202. The credit card 204, TAC 230, and transaction amount are then sent, via the direct dial network 240, to the Authorization Server 207. The Authorization Server 207 confirms with the card issuer 209 that the account has sufficient funds in the account and that the TAC co-relates with the user's PIN number and the issued security string 210. In the event that the account number, transaction amount, and TAC are verified the Authorization Server 207 allows the transaction to proceed.

In the second scenario, referred to as the merchant acquirer network scenario, the same initial steps apply. The user 201 receives a security string 210 which resides on the device 202, such as a mobile phone, and that when the user 201 is ready to purchase an item from the merchant 205 he or she, in step 220, presents the merchant 205 with the registered credit or debit card 204. The card 204 is swiped at the EFT/POS terminal and again the user 201 determines his or her four digit TAC 230, via the security string 210 residing on his or her mobile phone or device 202. In this scenario, the transaction information including the account number of the card 200 and amount of purchase are routed via path 250 to scheme 252. The standard credit card transaction details and the pre-authorized PIN are sent to the card issuing host server 209. The scheme 252 sends the card 204 information and pre-authorization PIN to the card issuer host 209 via communications path 256. At the

same time, the scheme 252 communicates with the Authorization Server 207 and verifies that the pre-authorized PIN correlates to the user's PIN. The card issuer 209 proceeds with the transaction and upon verification allows the transaction to proceed.

In addition to the dual channel schema described above, the present invention also allows for a single channel schema whereby a user would be able to use the present invention for such transactions as online purchasing via Internet websites. The single channel schema and protocol is conducted via either a computer, a WAP device, Smart Card, Proprietary System or a G3 mobile phone, where the security string is received and the TAC transmitted on the same device. This protocol does not require a secondary channel to conduct a secure transaction.

The single channel protocol runs via an applet downloaded by the user onto his or her computer, WAP device or G3 mobile phone. The security string and the TAC can only be received by an enabled server and transmitted via an SSL link. The present invention is resistant to 'ghost' sites, where the user is unaware that the site he or she is dealing with is not certified, because the merchant (whether certified or not) would only be in possession of the user's 'User name or card ID' and not the relevant TAC.

The single channel solution solves the problem encountered by transmitting the relevant TAC and security string over the Internet by instructing the users ISP (Web browser) to transmit only the user name to the merchant and the relevant TAC to the enabled server/database.

Figure 3 shows each step along the process a user would take to register and use the single channel schema. The process is started in step 300 and in step 310 the user contacts the server host of the present invention through a single channel device such as a personal computer, an internet connected hand held device, a cell phone or wireless phone, or any device that may support a web browser via a single communication channel. Upon contact with the server or host of the present invention a log on web page containing the interface applet is sent to the user's

device. In step two 320 the user is requested to input his or her user ID and preauthorized credit card or debit card number through an appropriate entry method. The user interface may include on screen drop down menus or other various user friendly applications to enhance the entry process of the user ID and credit card or debit card number. The user ID is sent to the server for verification. If the server verifies the user's identity a security string is sent to the client web page using the low processing overhead protocol (LPO protocol) with a prompt to initiate the applet. The applet is used to abstract and repack the TAC code according to the LPO protocol and start the Pin Safe interface.

In step 330 the Pin Safe interface is started enabling safe user entry of a PIN or TAC. The LPO protocol extraction is carried out using an automatic System Identification Digit (SID) and System Outgoing Digit (SOD) generation. As will be described in more detail below, the TAC code is pulled from the security string and repacked according to the LPO protocol and sent to the server host for verification. In step 340 the applet is stopped and destroyed, all values are zeroed and the security string residing on the device is cleared. The user sees an interface which identifies that the device is awaiting a response from the server. In step 350 the log on to the server is verified or rejected according to the user ID and TAC code response. If verified, confirmation is sent to the client browser followed by requested service access or transaction. In step 360 the session or transaction is finished allowing the user to close the session or the process or the session may be automatically closed triggered by some length of time of inactivity. The user's information with the single channel schema is terminated at step 370.

Figure 4 displays the main components for a preferred embodiment of the single channel schema of the present invention. The user 401 would visit the server 407 of the present invention and the server 407 would provide applets 470 for downloading to the user's device 403. The user 401 downloads an applet 470 via path 421 which is then stored on the device 403 as the customer applet 422. The web merchant 405 would also visit the Authorization Server 407 via path 450 and download the an

applet 470 via path 451 which is stored on the merchant site 405 as merchant applet 452. The user 401 using the device 403 visits the web merchant site 405 via path 430 and selects items he or she wishes to purchase by placing them in the basket 406 and selecting the appropriate credit or debit card for use 407. The merchant site 405 then accumulates the items in the basket 406, information about the card 407, and utilizing the merchant applet 452 routes the information along path 431 to the Authorization Server 407.

The Authorization Server 407 starts the verification process and using communications path 432 routes the appropriate information back through the merchant applet 452 to the customer applet 422 resident on the user's device 403. The user 401 is requested to enter the TAC. Once the user has entered the TAC, the TAC is sent along path 433 through the merchant back to the Authorization Server 407 to validate the response. In addition, the Authorization Server 407, at step 434, validates that there are sufficient funds in the account and in step 435 verifies that the information about the card 407, TAC, and account funds availability are verified. The Authorization Server 407 sends an "accept" notice along path 436 to the merchant site 405 which is then relayed, via path 437, to the users device 403.

Figures 5-7 also relate to single channel schemas utilizing different aspects and security protocols. In Figure 5, the user 501 visits a merchant Internet site 505 and would select various items for purchase. Upon checkout, payment is demanded via path 510 from the merchant site 505 to the user 501. The personal computer or device 503 contains an applet 522 which communicates with the site 505 and includes the proper software or applet 522 to notify, along path 520, the Authorization Server 507 that a transaction authorization is needed. The merchant domain name, transaction amount, user ID, and Transaction Authorization Code (TAC) are transferred from the user's device 503, along path 530, to the Authorization Server 507. Already present on the personal computer or user's device 503 is the security string for the user to determine his or her TAC code.

The Authorization Server 507 communicates with the merchant Internet site 505, via path 540, to certify the card and transaction amount information. The Authorization Server 507 also forwards a transaction ID via path 541 to the user 501 through the user's personal computer 503. The transaction ID is forwarded to the merchant's Internet site, along path 542, from the user's personal computer 503. The Authorization Server 507 certifies that the amount of purchase, the card information, and TAC are appropriate and sends the card details and amount along path 550 to the merchant Internet site 505. The transaction details are sent from the merchant Internet site 505 to the card issuer 509, via path 560, and ultimately the card issuer 509 sends payment via path 570 to the merchant Internet site 505.

The single channel schema displayed in Figure 6 is similar to the single channel schema displayed in Figure 5 except that a wireless device 604 is included to remove the security string from the user's personal computer 603. In the schema illustrated in Figure 6, the security string is omitted and simply the four digit TAC 620 for that transaction is transmitted from the Authorization Server 607 to the user's wireless device 604.

Figure 7 is a single channel schema similar to the single channel schemas disclosed in Figures 5 and 6 except that instead of the four digit TAC being transmitted from the Authorization Server 707 to the wireless device 704, as described above in relation to Figure 6, a thirteen digit security string 720 is sent to the wireless device 704. The schema disclosed in Figure 7 discloses that as the user 701 selects items to be purchased from the merchant internet site 705 the payment demand along path 710 is sent to the user via the user's personal computer 703. The applet 722 then prompts the user to enter the TAC code, which the user determines from the security string 720 sent from the Authorization Server 707 to the wireless device 704. The applet 722 forwards the merchant domain name, transaction amount, user ID, and TAC to the Authorization Server 707 along path 730. The Authorization Server 707 certifies the transaction, along path 740, and forwards the user account number and amount along path 750 to the merchant Internet site 705 . The transaction details are sent

from the merchant internet site 705 to the card issuer 709, along path 760, and payment is then forwarded from the card issuer 709 to the merchant internet site 705 along path 770.

In the various online merchant scenarios employing the single or dual channel schema, as seen in Figures 2-7, there may be instances when the merchant does not have a particular item in stock and therefore can not process or complete the entire transaction immediately. In these instances, the merchant typically does not complete the transaction until the merchandise is dispatched. However, the user may have already input his or her TAC and the system would want to send the user a new pseudo-random security string.

The present invention overcomes this hurdle by having the Authorization Server receive the payment request and the active TAC. The merchant's server typically would transmit the order request to the authorisation server within a nominal 1-minute time out. However, if the merchant has received a purchase order for goods not in stock that order request will be delayed. The delayed order request will not be sent to the authorisation server until the goods have been received and are ready to be dispatched to the customer. Upon reception of the user's TAC and transaction details and the absence of the merchant's transmission of the order within the 1-minute timeframe the authorisation server will default to a deferred payment program.

The deferred payment program will hold the active TAC at the Authorization Server and is proof that the user has ordered the goods. A new security string can then be issued to the user for use during the next transaction. The authorisation server program will immediately send an email to the user stating details of the goods that he or she has requested from the merchant. Every week, or some other predetermined time interval, the Authorization Server will remind the user of his or her order request. The user is therefore informed of any pending transactions that will be eventually cleared through his or her account.

When the goods arrive at the merchant's depot and are ready to dispatch, the merchant details are then transmitted to the Authorization Server and the transaction is completed. If by this time the user has insufficient funds to cover the transaction amount the transaction would be declined, as typical in a standard credit card transaction.

Figure 8 represents an additional schema utilizing features of the present invention in which a user has a pre-authorized or debit account 804. The user would see a live device 805, such as a vending machine, and would select items via path 810 thereby triggering the live device 805 to demand payment. The payment demand would be routed through the pre-authorized liquid account 804 which is done by swiping the pre-authorized account 804, such as a credit or debit card, in step 840 through a card swipe device 806. In addition the micro payment demand would also notify the card swipe device 806 that a TAC would be requested. The user may have a personal device 803, such as a wireless phone, which would contain either a TAC or security string whereby the user would determine the TAC and enter the TAC 830 into the card swipe device 806. Alternatively, the user could enter the TAC 830 into the wireless device 803 which would wirelessly transmit the TAC 830 to the card swipe device 806 or Authorization Server 807 . The details of the transaction are sent along path 850 from the card swipe device 806 to the Authorization Server 807. The Authorization Server 807 contains the information on the liquid account and if verified would notify a micro payment host 808 along path 860 to authorize payment. The micro payment host 808 then transfers payment along path 870 to the live device 805.

Figure 9 represents a data control schema whereby elements of the present invention can be used to add a security overlay and pre-authorization into a database for controlling access to a database. In Figure 9 the user 901 through his or her computer or laptop 903 wants access to a database 909. Access is requested along path 910 from the Authorization Server 907. A security string is sent from the Authorization Server 907 to the computer 903, via path 920, whereby the user determines his or her

TAC. The user inputs the TAC which is transmitted to the Authorization Server 907 along path 930. Provided the TAC matches the appropriate PIN verified for the user 901 the Authorization Server 907 allows access to the database 909 along path 940. Further, the system can simply transmit the TAC, instead of the security string. The access data is then transmitted to the user's computer 903 through the Authorization Server 907 via path 950. In addition, the security string can be sent to the user 901 via an alternate path 921 such as through use of a wireless device 904.

Figure 10 represents a remote bank balance inquiry schema whereby a user can check the balance of an account. In the schema presented in Figure 10, the user 1001 through use of a cell phone, pager, or wireless device 1004 can request the balance of an account located in a bank 1008. The user is provided with a security string or TAC, via path 1010, which is resident on the wireless device 1004. The user determines his or her TAC code and either presents his or her TAC code through a bank teller (not shown) or inputs it into the wireless device 1004. The TAC code is sent to the Authorization Server 1007 which verifies that the TAC code is appropriate for the security string and corresponds with the user's PIN. The Authorization Server 1007 then communicates with the bank 1008 along path 1020 to retrieve the account information thereby providing the user with the requested information.

Two important aspects of the present invention which are utilized in the dual and single channel schemas described in relation to Figures 2-10 are the low processing overhead protocol and the security string operation. Certain wireless devices, such as web devices, cannot run high level encrypted programs due to their low processing overhead. The present invention incorporates a low processing overhead protocol which enables such devices to run highly secured transactions or downloads without using a large memory foot print. An additional benefit of the low processing overhead protocol is that existing transaction data issuing servers could also process information quicker than traditionally encrypted systems. The low processing overhead protocol evades the possibility of a correlation between the TAC and security string by simultaneously using multiple security strings. Only one of the

multiple security strings is actually relevant and the remaining strings are used to hide the relevant string. The security strings contain identical digits but are arranged in different random orders. The user's applet receives the multiple security strings and distinguishes which string is relevant by using a system identifying digit (SID). The system identifying digit knows which of the security strings is genuine and instantly dumps the irrelevant strings and processes only the correct and relevant string. As an example, if the identifying digit value was 4, the present invention would identify that the fourth security string was the relevant security string.

During a transaction, as will be described in conjunction with Figures 11 and 12, the user inputs his or her PIN and the TAC is internally calculated on the applet of the wireless device, personal computer EFT/POS, or as seen in Figure 11, a thirteen digit security string 1100 would be sent from the Authorization Server to the user's device identifying a string of random digits, in this instance thirteen (13). The security string 1100 may come with a two letter identifying prefix 1101 which identifies which server has issued the security string 1100. For example in Figure 11, if the user's PIN was 2468 and the user applies that PIN number to the digit locations in the security string 1100. The user would look at the number in the second spot, the fourth spot, the sixth spot and the eighth spot to determine his or her transaction affirmation code or TAC for that particular transaction. In this instance, the user's PIN of 2468 would yield a TAC of 7693. Therefore, the user would input 7693 as the TAC to notify the Authorization Server to continue with the verification process.

Further explanation of the manner in which the TAC is secured within the transmitted secure security strings is explained in conjunction with Figure 12. As seen in Figure 12, the user, or customer 1201 has a known PIN 1202 (i.e. 1234). Stored on the user's device and downloaded from the server 1207 is the thirteen digit pseudorandom string 1203. In this instance, the customer's PIN value of 1234 as it relates to the pseudo string 1203 indicates a TAC code 1204 of '6891.' When the user is asked to verify or input the TAC 1204 to authorize the server 1207 to verify that the customer 1201 is in fact the authorized and registered customer the TAC

1204 may be manipulated and reversed in a myriad of ways to protect the code during transfer along the communications path to the server 1207. One method for providing a security overlay to the customer's PIN 1202 and the TAC code 1204 is to incorporate the TAC code into one thirteen digit string of a multitude of strings as previously described.

To identify the appropriate string the applet running on the customer's device would identify the relevant string through a system identifying digit 1205. The SID 1205 is used to identify which of the security strings is relevant. The SID 1205 may be determined in a myriad of ways including using certain numbers or combination of numbers of the user's PIN 1202, having the user set the SID 1205, and having the system server set the SID 1205. In the example shown in Figure 12, the system set the SID value equal to 3. Therefore, the third string of nine strings is the relevant string. The nine (9) strings of thirteen (13) digits are sent via a data connect, such as a data stream 1230, to the user or customer's 1201 device. The applet on the device knows the SID 1205 value and extracts the relevant string 1203.

The customer reviews the relevant string 1203 resident on his or her device and determines his or her TAC 1204. The TAC 1204 is then intertwined into an outgoing relevant string which is grouped with eight (8) non-relevant strings. The outgoing data stream 1240 contains nine outgoing strings of thirteen digits. The location of the relative outgoing string is identified by a system outgoing digit (SOD) 1209 which can also be determined in a myriad of ways such as using or adding certain numbers of a customer's PIN 1202 or having the customer or system server select the SOD 1209.

In this example, the system set the system outgoing digit (SOD) 1209 value at 2. Therefore, the TAC 1204 will be integrated into the second of nine strings in the data stream of strings 1240. The TAC code 1204 may also be inversed, manipulated, have an automatic number added to it (i.e. each number is increased by one), or any other manner in which the PIN number can be modified prior to transmission. In the

example shown in Figure 12, the TAC code 1204, is inversed to determine the location of the TAC numbers within the relevant outgoing string. For example, since the TAC 1204 in this example had a value of '6891' the inverse value of '1986' would dictate that in the first spot is the first digit of the TAC code, in the ninth spot is the second digit of the TAC and so forth until the TAC is integrated into the relevant security string.

The data stream of outgoing security strings 1240 containing the nine strings of thirteen digits is sent to the server 1207 which has an applet for verification. The server 1207 has an applet which knows the SOD 1209 value and can identify the relevant outgoing security string for verification of the user's PIN. Therefore, the applet on server the server 1207 knows the customer's PIN 1202 is '1234' and can determine that based upon the protocol established can determine that the SOD 1209 value was 2 and therefore the relevant string is the second string. The server 1207 will analyze the second string in relation to the user's stored PIN and expected response to verify that the response matches the TAC 1204 code from the initial string 1230.

Upon receiving the nine carrier strings, the server 1207 knows the outgoing digit position of the relevant TAC carrier string and instantly dumps the irrelevant strings and processes the correct selected TAC carrying string. The verification process at the server 1207 then matches the correct TAC with the issued security string and user's PIN number. If all three correlate, the authorization is completed and a new security string is transmitted to the user's applet.

Although in this example the number has been limited to nine lines of thirteen digits plus three (3) system digits per line (totalling 144 digits). It is not meant to limit the number of lines or digits that can be used. The nine lines of thirteen digits totalling 144 digits is intentionally less than the total global packet standard for many devices of 160 characters. Therefore, keeping the digit size below 160 keeps the processing overhead at a minimum allowing for low processing capability in WAP applications

and wireless devices. In addition, this low processing overhead results in extremely fast verification times. The verification process also employs a filtering step followed by a single dimension array process which is not an intensive arithmetic computation system which would require more processing time.

In addition to the various single and dual channel schemas, the low processing overhead protocol, and use of the multiple security string security overlay the present invention may also provide a security overlay within the user interface. Figures 13a-13h represent various user interface examples to which a user may be provided for inputting a user's TAC . In the examples provided in 13a-13h the user would remember his or her personal PIN as a pattern rather than a numerical sequence. As an example, if the user had chosen to use the shape 1301 and shown display in Figure 13e, they would only have to remember that they created a PIN which creates a small box 1303 inside of the shape 1301 disclosed in Figure 13c. When the display is populated with random numbers then the user applies his or her chosen design (i.e. small box 1303). In this example, the user's PIN from box 1303 would be '2389'. Therefore, knowing the PIN of '2389' and viewing the randomly generated numbers within the random display 1302 the user would see that the numbers '7538' correspond with his or her PIN number location. Therefore, the user's TAC for completing such a transaction or entry into the database, would be '7538'. The user interfaces disclosed in Figures 13a-h are merely exemplary and numerous displays, as well as colours and graphic symbols could be incorporated into the user interface. Therefore, the user would be able to create a graphic representation of his or her PIN without the need to remember the four digit PIN number.

Another feature of the present invention which deals with the user interface of the system involves the use of a Pin Safe deterrent interface. Any device with a keyboard or touch sensitive interface which may be connected to a network or which is otherwise capable of downloading data or machine code may have the integrity of a password or key entry security system comprised. One way in which the system may be comprised is through the use of a Trojan program. A Trojan program is a

small program which collects keyboard information for latter use. An additional program can also collect password or key entry information but feigns an unsuccessful logon attempt at the last digit of the logon entry and attempts to continue the logon with the real user unaware, by guessing the last digit (this is known as a "sniffer" program). Both of these techniques require actual data from a device keyboard or key pad or other input device. Whereas data may, by encryption or other means, be delivered and resent securely right up to and from the actual process occurring in the devices processing unit, if the security system requires meaningful user data entry to access or operate the security system that data may be intercepted and relayed greatly reducing the security of the system.

Although keyboard or small amounts of other input data may be redirected or stored with little or no user indication or system performance impact the same cannot be said for the device's graphical display, where the output is high throughput and device specific. Screen grabbing, or screen capturing, is possible but system resource intensive and therefore quite likely to be discovered by a user, especially on a device of comparatively low processing power. A good level of resistance could therefore be offered by an interface that provides information to a security system that is only meaningful to that system within the scope of its own time interface parameters and where any captured keyboard information has no external meaning. Similarly, any possible screen grabbed or screen captured information should not compromise the system's logon security.

The inputting of a Username, Password or PIN number in a computer, PDA, 2.5G or 3G mobile device is currently flawed for the following reasons: (1) the User can be seen by onlookers entering his or her PIN number into the device (called 'shoulder surfing'); (2) the keyboard could contain a 'Trojan' program that records the inputted Username, Password or PIN number (Trojans are downloaded without the knowledge of the User onto a computer and can reside there indefinitely); (3) PKI Certificates authenticate that the transaction was conducted on a certified computer, but they do not effectively authenticate the User behind the computer; and (4) computers running

Microsoft Windows have a problem because Windows remembers the Username, Password or PIN number which creates a situation where the device stores the I/D of the User within the computer.

The "radar" deterrent or Pin Safe user interface of the present invention achieves a positive user I/D because the user has to be present during every transaction. The Pin Safe user interface is Trojan resistant because any key can be used to input a PIN or TAC which renders any Trojan key intercept information useless, as does the displayed information on screen.

In addition, the user interface is shoulder surfing resistant because there is nothing that could be gleaned from looking either at the screen or the keyboard input, rendering shoulder surfing a pointless exercise. Further, the system is resistant to PIN interception when using the Dual and Single channel (Applet) protocol. The protocol of the present invention is unique because it transmits a volatile TAC every time a transaction is made. A successful attempt to intercept/decrypt this information could not result in the user's real PIN being compromised.

Another feature of the present invention is that it is a multi-platform system. The PIN Safe user interface works on a wide variety of computers and applications because of its low memory footprint and simple generic user interface. The protocol and system as a whole is non device-specific and can run on any device such as a public use computer. The system does not have to run on a trusted computer system where the program history is known. With no digital certificate required for the computer the User could conduct a transaction on any computer worldwide.

Further, the user interface is easy to use because the user need know nothing about the protocol, TACs and Security Strings. The PIN Safe user would merely input his or her unchanging PIN via the Pin Safe user interface. Further, the Pin Safe user interface is "tempest" proof because the interface does not display the users PIN or TAC (Pseudo PIN) on screen, and therefore is not subject to Electro-magnetic

emissions from the VDU that could be the subject of surveillance via Tempest technologies. The strong protection gained by using the Pin Safe user interface of the present invention allows safe single PIN usage on a variety of accounts with differing security architectures which can be achieved by using a central PIN Authorization Server. Even if the security string resides on the device it is not a problem because the present invention does not require a digital certificate and therefore there is nothing in the memory of the computer that compromises the User's I/D if it falls into the wrong hands.

The Pin Safe user interface involves a unique method of inputting a PIN number into a computer, ATM, PDA, 2.5G or 3G Mobile Device. Figures 14 and 15a - 15e are representative examples of the Pin Safe user interface screens. When a user wishes to conduct an online transaction, the Pin Safe applet will activate which will provide the "Start" user interface displayed in Figure 14. Pressing any key on the user's computer screen TAC or PIN then activates the entry interface screen. The interface can be activated by using the keyboard, mouse, or a touch screen display.

As seen in Figures 15a – 15e, the Pin Safe interface will now start to display (in this example in a clockwise manner) 12 digits in sequence (starting with 1 and ending in 12). During the display cycle, the User simply registers his or her PIN or TAC by pushing any key on his or her keyboard, mouse or any spot on the touch screen display when the digit they wish to register is illuminated. The Pin Safe display will rotate 4 times, once for every digit of a 4 PIN number.

At the 12^{th} position there is a dwell time to allow customer response for the starting of the next cycle accurately. When the first cycle for the first PIN number has finished the display will start again with another cycle. The cycles can also be identified by changing the illumination colour. This process is repeated 4 times until all 4 digits are inputted to make up the User's 4 digit PIN.

For example, as seen in Figures 15a - 15d, if the user's PIN was '2468' then on the first cycle the keyboard would be pressed when the 2nd digit was illuminated, see Figure 15a. On the second cycle the keyboard would be pressed when the 4th digit was illuminated (see Figure 15b), on the third cycle the keyboard would be pressed when the 6th digit was illuminated (see Figure 15c), and on the fourth cycle the keyboard would be pressed when the 8th digit was illuminated (see Figure 15d). Only one display is seen at any one time on the screen preventing an onlooker from determining which PIN is being inputted. Further, the changing colours of the display background and the digits displayed can be pseudo-random.

After the User presses the keyboard to register the first PIN TAC digit a random run on period of time is activated. The run on process prevents shoulder surfers from seeing exactly which digit was registered. For example, as seen in conjunction with Figure 15a, when the User wishes to register the first digit, as number 2, they would press any key on the keyboard when the number 2 or second digit is highlighted, however the display continues illuminating the numbers or digits after 2 around the cycle. The system may also illuminate only a portion of the numbers after the selected number, such as between 0 to 4 digits after the selected number, before speeding up the illumination of all numbers until completion of the cycle. A shoulder surfer would see the cycle speed up after the numbers 2,3,4,5 or 6 were illuminated and would not be able to determine which digit had been registered. After the run on period, the system may increase the cycle speed to complete the cycle so that the user does not have to sit through the full cycle time to aid quick PIN entry. The run on period is normally less than the point in elapsed time from the key press to the time when the user would start to question whether a positive selection had been made. For short term visual memory, of a human, this is a maximum of around three seconds.

The run on period and increased cycle speed may be applied on all 4 cycles or displays. The dwell time between the digits being illuminated and the change in cycles is pseudo-random to prevent Trojan programs from determining which digit

was inputted by correlating the display with the keyboard and the user's computer clock speed.

As seen in Figure 15e, the Pin Safe user interface can also use characters, letters, or symbols instead of numbers on the display which would allows the user's code or pin to be any group of symbols or letters which spell a word. In addition, as previously discussed, in relation to Figure 9, the present invention can be used for the remote access of data using either the Dual or Single Channel schema or protocol and the PIN Safe interface.

Enabling an existing database with the PIN Safe interface of the present invention can be done by providing an authentication server computer that registers the User's PIN number, issues and stores security strings, and correlates the received TAC to authenticate the user's identification.

In addition, the Pin Safe or Radar Interface can work within a computer's own processor, within a LAN configuration, and over the Internet. Operating within a computer's own processor the Pin Safe interface could act as a hack proof screensaver which means that when a user first started his or her computer he or she will be presented with the interface. The user must input his or her PIN accordingly and if the user decided to leave the computer for a short time, where there is the opportunity for criminal use of his or her computer, the user could press a function key which would activate the Pin Safe interface. Upon returning to his or her computer he or she would simply click on his or her mouse or any key and enter his or her PIN via the Pin Safe interface.

In addition, if a user fails to input his or her PIN digit during any of the 4 sweep cycles, the present invention will allow the input of the PIN digit during any sweep (provided they are in the correct sequence). This means that a 'Reset' button will not require pushing unless the user has made a conscious mistake.

Additional schemas for employing the security features, measures, protocols, interfaces, and overlays of the present invention are discussed in connection with Figures 16-23.

As seen in Figure 16, the Authorization Server 1607 is connected directly to a Client's Host Gateway Server 1609. The Host Gateway Server 1609 is the database's 1611 connection to the Internet 1613 and it is placed outside the firewall 1615 that surrounds the host database 1611 (this is to ensure that any hacking activity cannot occur inside the database 1611). The remote data access configuration may also employ the Pin Safe interface 1623 in conjunction with the user 1601 and the user's device 1604. The system may also employ a backup server or database 1630.

The Authorization Server 1607 can be configured to act as dual or single channel system. Its architecture allows the Host Gateway Server 1609 to allow access to the database 1611 either via the present invention or via its existing access procedure. This means that after installation, the enabled access trials can be conducted without affecting the original configuration.

Figure 17 shows how multiple Clients 1740, 1750 can be accessed from one User 1701, using one PIN number. This is achieved by installing a Central PIN Authorization Server 1707 which consolidates the received TACs with the issued security strings from any enabled Client 1740, 1750.

The Pin Safe interface can be applied various ways including the dual channel, single channel: Thin Client and single channel Applet embodiments. In the dual channel application as seen in Figure 18, the User's TAC is inputted via the Pin Safe interface 1823 and it is sent directly to the Authorization Server 1807 through the Internet 1813. With the dual channel application no security string is sent to the User's computer 1822 and instead it is sent to the mobile device 1804 via SMS.

As seen in Figure 18, the Security String is sent from authorization computer 1807 to the User's mobile device 1804. The user inputs the TAC via the Pin Safe interface 1823 and the Authorization Server 1807 receives the TAC via the Internet 1813.

In the single channel Thin Client application, as seen in Figure 19, the Pin Safe interface applet 1923 resides on the Authorization Server 1907. The User 1901 accesses this applet 1923 remotely from any computer 1922 and does not need to 'set up' the computer 1922 by pre-downloading any form of program beforehand. As seen in Figure 19, the User accesses the Authorization Server 1907 and applet 1923 via the Internet 1913. The User 1901 inputs his or her PIN, which is correlated at the source or Authorization Server 1907.

In the single channel Applet application, as seen in Figure 20, the Pin Safe interface applet 2023 resides on the user's computer 2022. The applet 2023 needs downloading only once and would be automatically sent to the user's computer 2022 during the registration process. The Pin Safe interface has been specifically designed with an extremely small memory footprint making the process of downloading and use very fast.

As seen in Figure 20, the User accesses the Authorization Server 2007 via the Internet 2013. The user 2001 inputs his or her PIN, which the applet 2023 converts into a TAC (it does this automatically using the volatile security string resident in the applet 2023) and then sends, via the Internet 2013, for correlation at the Authorization Server 2007.

Figure 21, shows a typical data access application where an Authorization Server 2107 has been fitted to a Gateway Server 2109 accessing a Database 2111. Figure 21 assumes that the user 2101 has registered with the system and has the Pin Safe Interface applet 2123 on his or her computer. To access information from the Database 2111 the Authorization Server 2107 sends a new security string to the user's computer or G2 mobile phone 2104 via the Internet 2113 or through a wireless

connection 2151. The security string 2151 resides on the device 2104 until the user 2101 wishes to access the Database 2111.

The User 2101 sends his or her volatile TAC to the Authorization Server 2107 to confirm his/her identity. In the dual channel scenario the user obtains his or her TAC from the G2 mobile device 2104 via either visual extraction (using his or her PIN as a sequencer) or SmartPIN or SIMM extraction where the User 2101 enters his or her PIN into the device 2104 and the relevant TAC digits are displayed on the device 2104 screen. The TAC is then inputted into the user's computer (not shown). In the single channel scenario the user simply inputs his or her PIN into the Pin Safe interface 2123. The PIN is then converted into a TAC within the applet 2123 and transmitted via path 2120 to the Authorization Server 2107.

Only when the user's identification is positively confirmed, by correlating the received TAC to the user's PIN and previously issued security String is the request 2130 for data, via the Gateway Server 2109, initialized via path 2130. The requested data can now be routed via path 2140 to the user's computer.

The Pin Safe interface is not required if the security string delivery and TAC extraction are conducted on a second device such as through the dual channel protocol. Using a G2 mobile phone a user can receive a security string and extract the TAC independent of the data accessing computer. This means that the TAC can be entered into the data accessing computer without the requirement of the Pin Safe interface because a TAC is inherently secure against shoulder surfing, Trojans, Tempest technologies and online user identification theft.

Figure 22 displays a generic Server/Gateway Schema incorporating various aspects of the present invention. The generic secure server schema may also incorporate UPS (Un-interruptible Power Supply), Dual Redundancy, Disk Mirrored, Linux Web Server 2245 and Internal Firewall 2215, the Pin Safe applet 2223, a user database 2207 and an internal maintenance any reporting function 2211.

Figure 23 shows the Generic Integration Platform which displays the Authorization Server 2307 inside a firewall 2315. The Authorization Server 2307 is connected to a Net Server 2317 and a host database 2311. The host database 2311 may also be inside its own firewall 2316.

Additionally the authorization process identifies the user via a response rather than an identifying account and its parameters which negates the so called "Friendly Fraud" from misuse of online fraud guarantees. An added benefit is that there is also an audit trail for database files access.

Any reference herein to a computer means any personal computer, ATM, PDA, G2.5 Mobile Device, G3 Mobile Device, or any device with a CPU. Any reference herein to a transaction means any financial transaction, remote Data Access procedure, or any interface transaction between a user and a system. The numbers on the various user interfaces and displays are merely exemplary and the use of characters, letters, colours and such may be used individually or in combination and still fall within the intended scope of the present invention.

In the present specification and claims, any occurrences of the word "comprising" and its derivatives, such as "comprises" and "comprise", are to be constructed in a non-exclusive sense rather than in the exclusive sense of the phrases "consisting of and only of", "consists of and only of" and "consist of and only of" respectively.

While the preferred embodiment and various alternative embodiments of the invention have been disclosed and described in detail herein and by way of example, it will be apparent to those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope thereof, and that the scope of the present invention is to be limited only by the following claims.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for verifying the identity of a user having a personal identification number (PIN), the method including the steps of:

i) forming display characters on a display of a computational device, the display characters being in correspondence with characters comprising the PIN to assist the user to input a volatile identification code derived from said PIN; and

ii) verifying the identity of the user on the basis of the volatile identification code.

2. A method for verifying the identity of a user, wherein the user has a personal identification number (PIN) comprising a first array of numbers, each number having a given numerical position in the first array, the method including the steps of:

i) forming a second array of display characters on a display of a computational device, each display character having a given numerical position in the second array;

ii) processing a volatile identification code input by the user upon application of the PIN to the second array; and

iii) verifying the identity of the user by checking that the volatile identification code matches a third array of characters formed by sequentially selecting display characters at numerical positions in the second array on the basis of the numbers in the first array, taken in positional order.

3. A method according to claim 1 or claim 2, wherein the display characters comprise letters of the alphabet.

4. A network server programmed to implement a method according to any one of the previous claims.

5. A method for verifying the identity of a user, substantially as hereinbefore described with reference to any one of Figures 1, 11, 12 or 13 of the accompanying drawings.

SWIVEL SECURE LIMITED

DATED THIS 2nd DAY OF JUNE 2005
BY MY ATTORNEYS
EAGAR & BUCK PATENT AND TRADE MARK ATTORNEYS

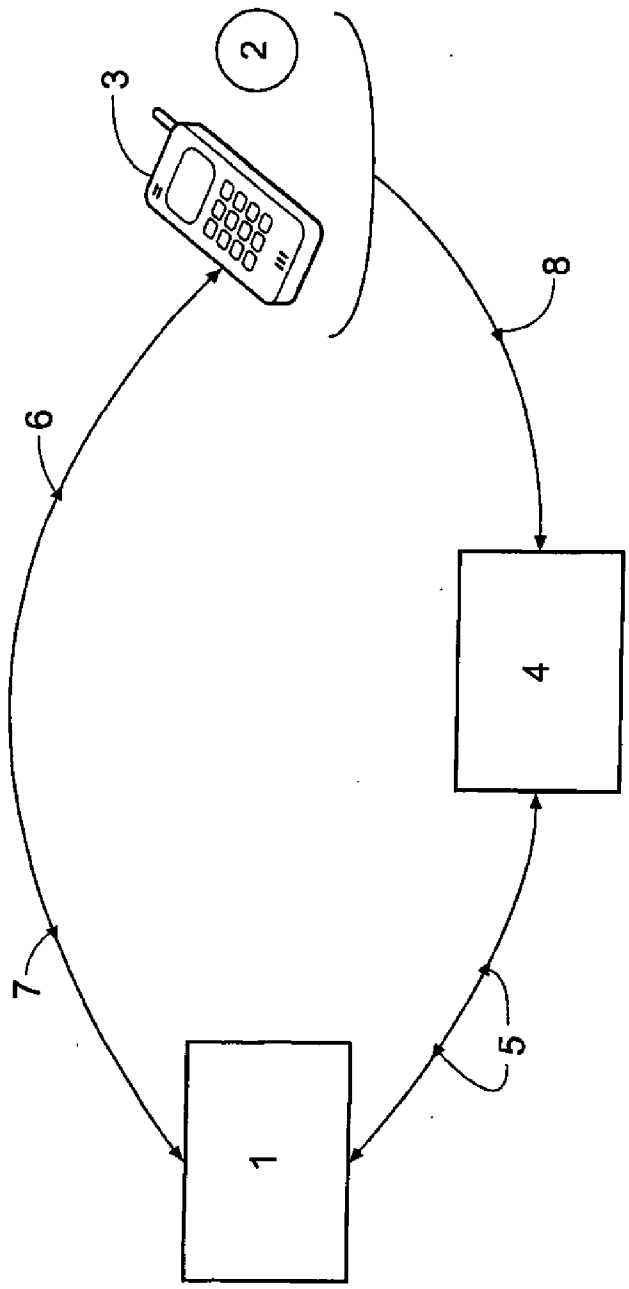

Fig. 1

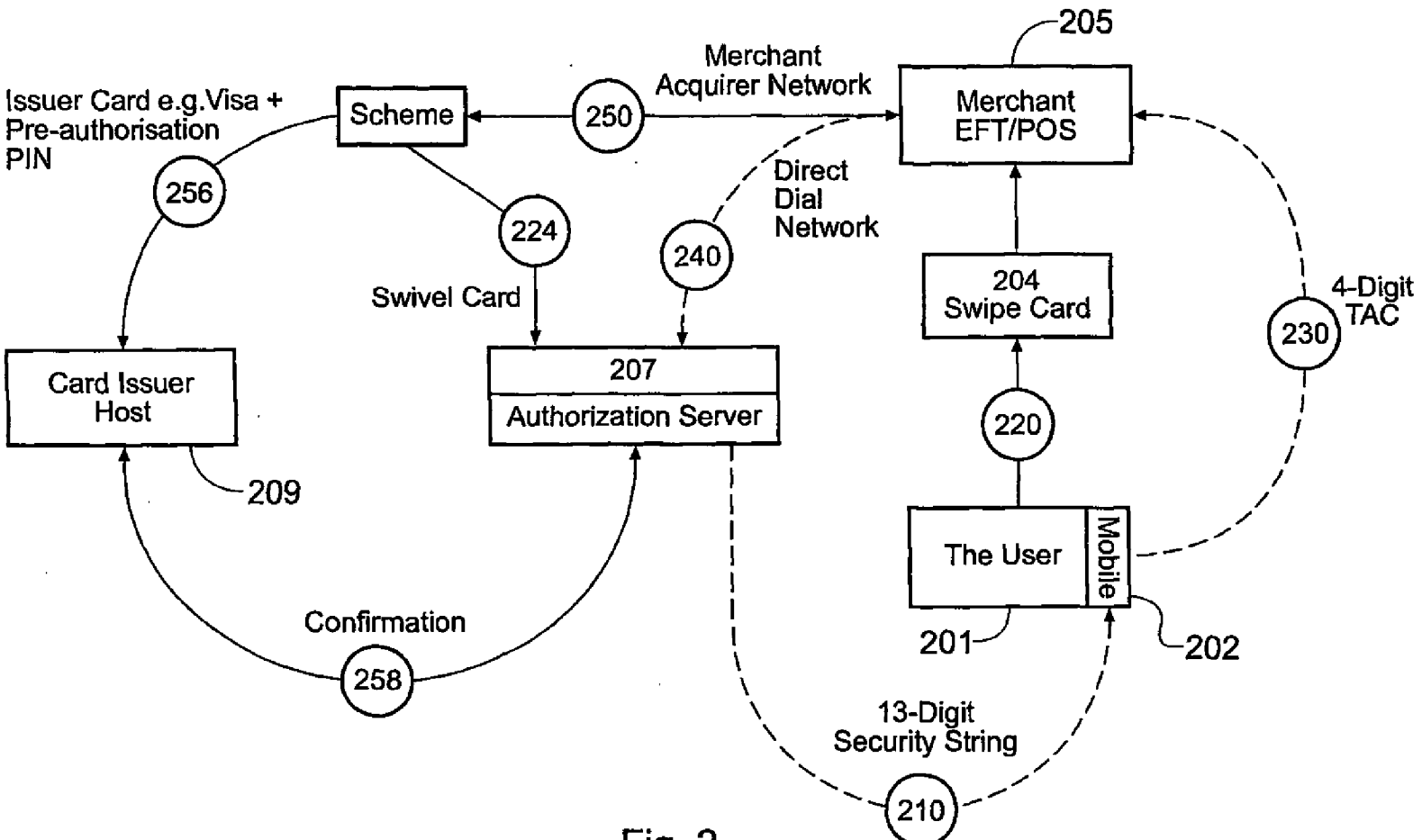
205
Merchant
Acquirer Network
Issuer Card e.g.Visa +
Pre-authorisation
PIN
Scheme
250
Merchant
EFT/POS
256
224
Direct
Dial
Network
240
Swivel Card
204
Swipe Card
4-Digit
TAC
230
207
Authorization Server
Card Issuer
Host
220
209
The User
Mobile
Confirmation
258
201
202
13-Digit
Security String
210

Fig. 2

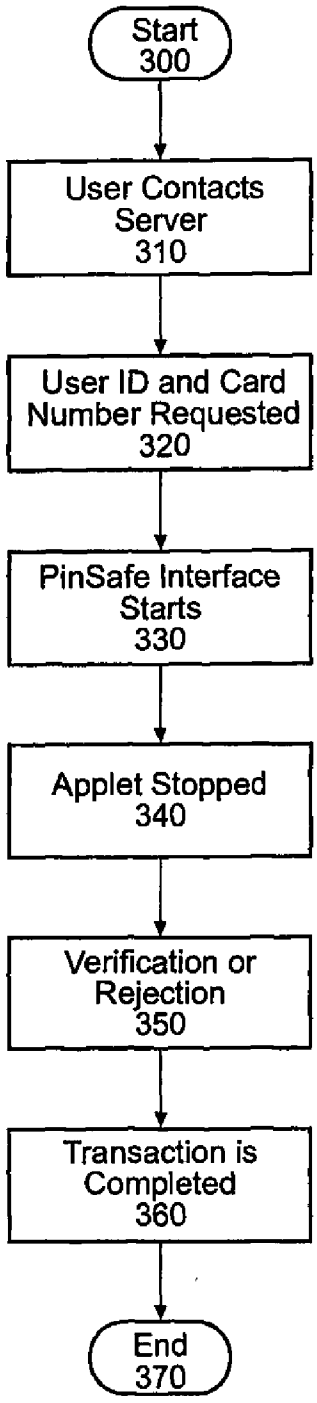

Fig. 3

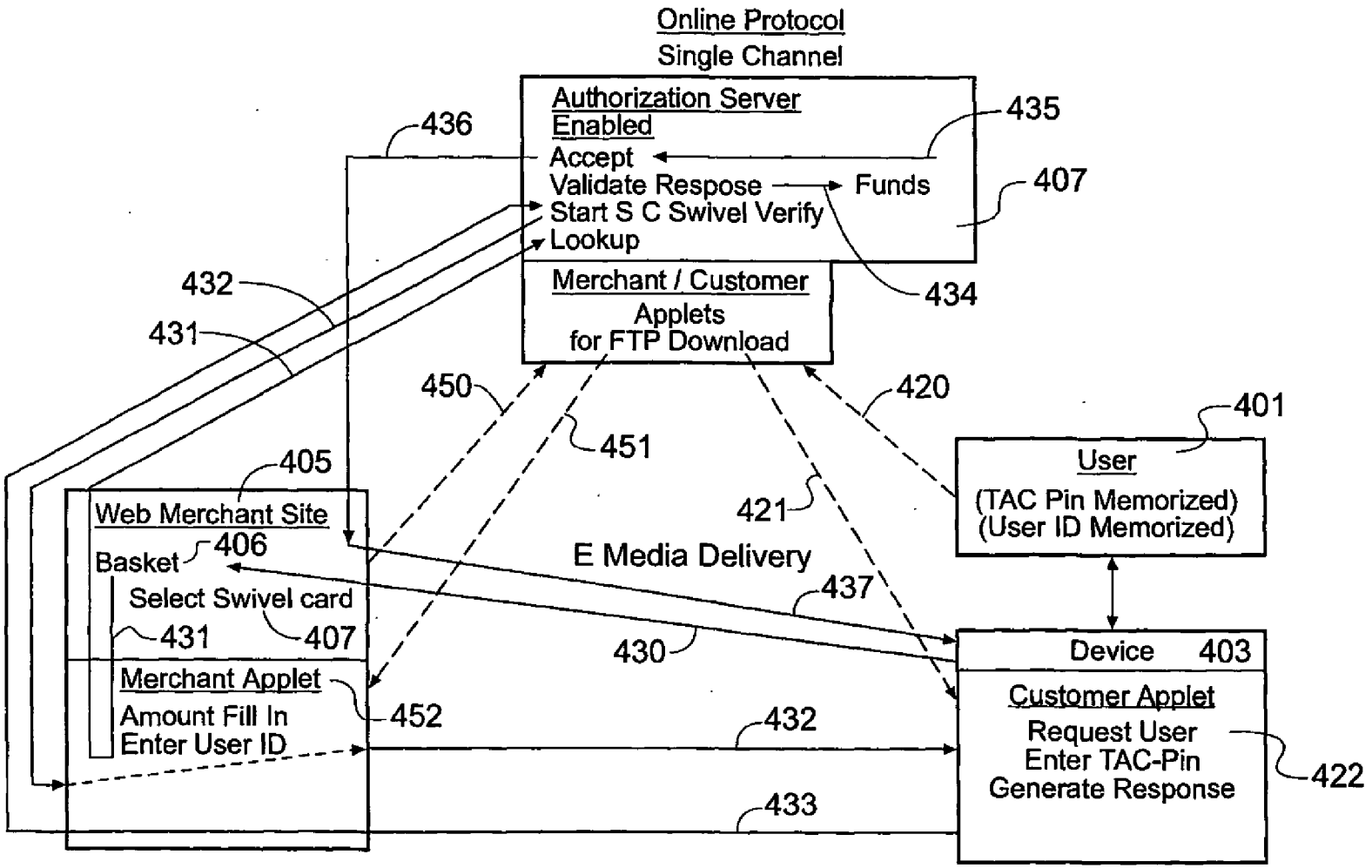

Fig. 4

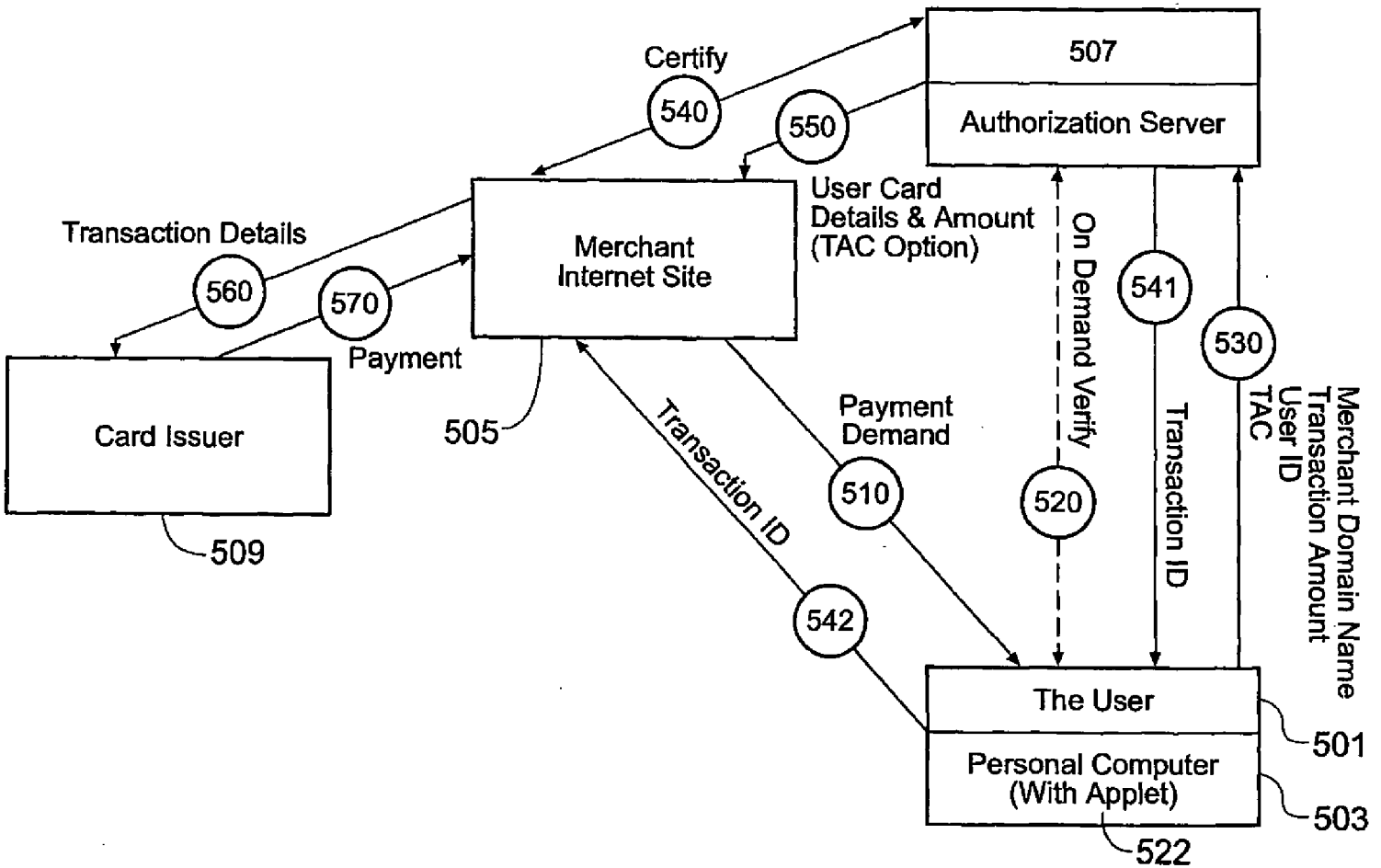
507
Authorization Server
Certify
540
550
User Card
Details & Amount
(TAC Option)
Merchant
Internet Site
Transaction Details
560
570
Payment
Card Issuer
509
505
Transaction ID
542
Payment
Demand
510
On Demand Verify
520
541
Transaction ID
530
Merchant Domain Name
Transaction Amount
User ID
TAC
The User
501
Personal Computer
(With Applet)
503
522

Fig. 5

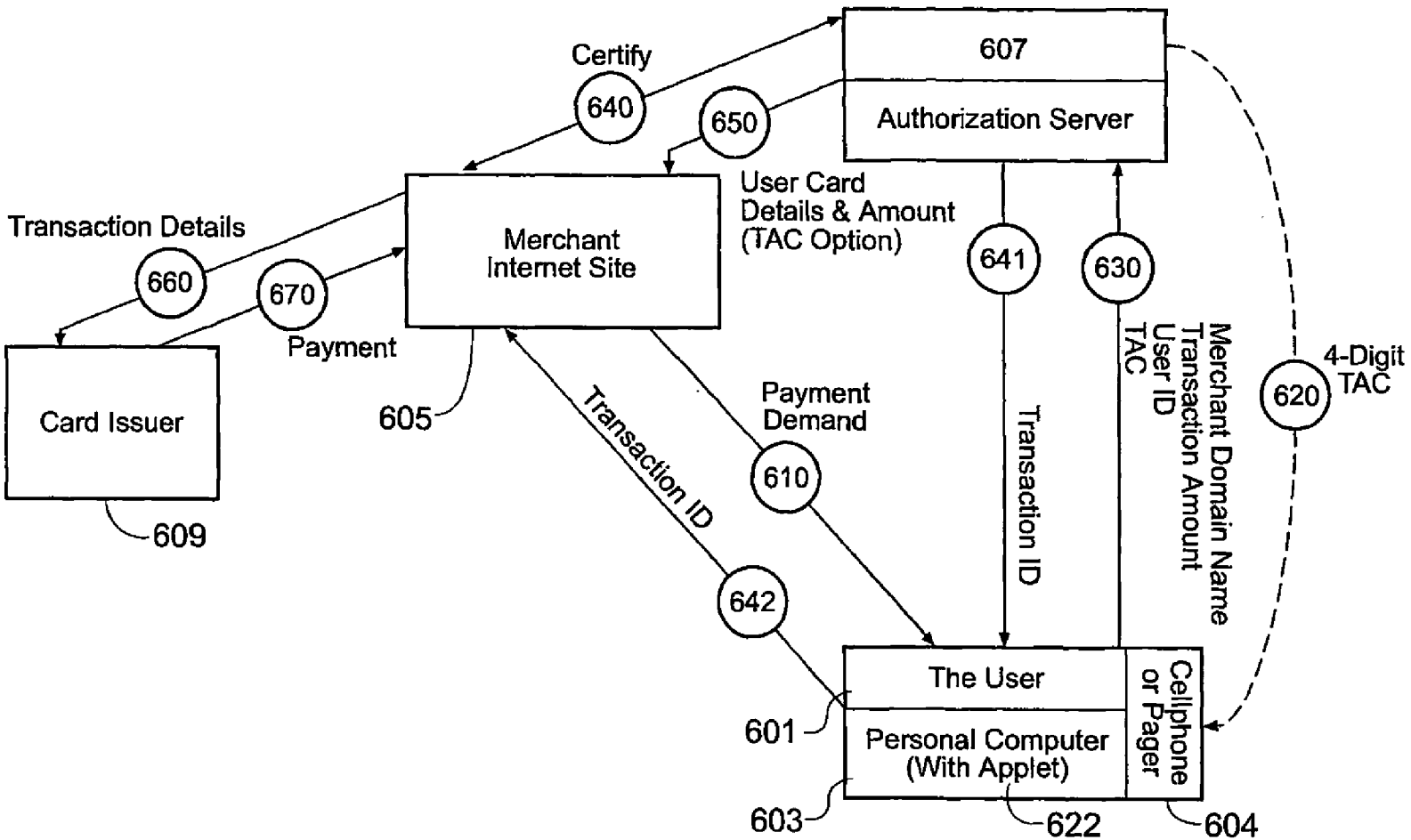
607
Authorization Server
Certify
640
650
User Card
Details & Amount
(TAC Option)
Merchant
Internet Site
Transaction Details
660
670
Payment
605
Card Issuer
609
Transaction ID
642
Payment
Demand
610
641
Transaction ID
630
Merchant Domain Name
Transaction Amount
User ID
TAC
620
4-Digit
TAC
The User
Personal Computer
(With Applet)
Cellphone
or Pager
601
603
622
604

Fig. 6

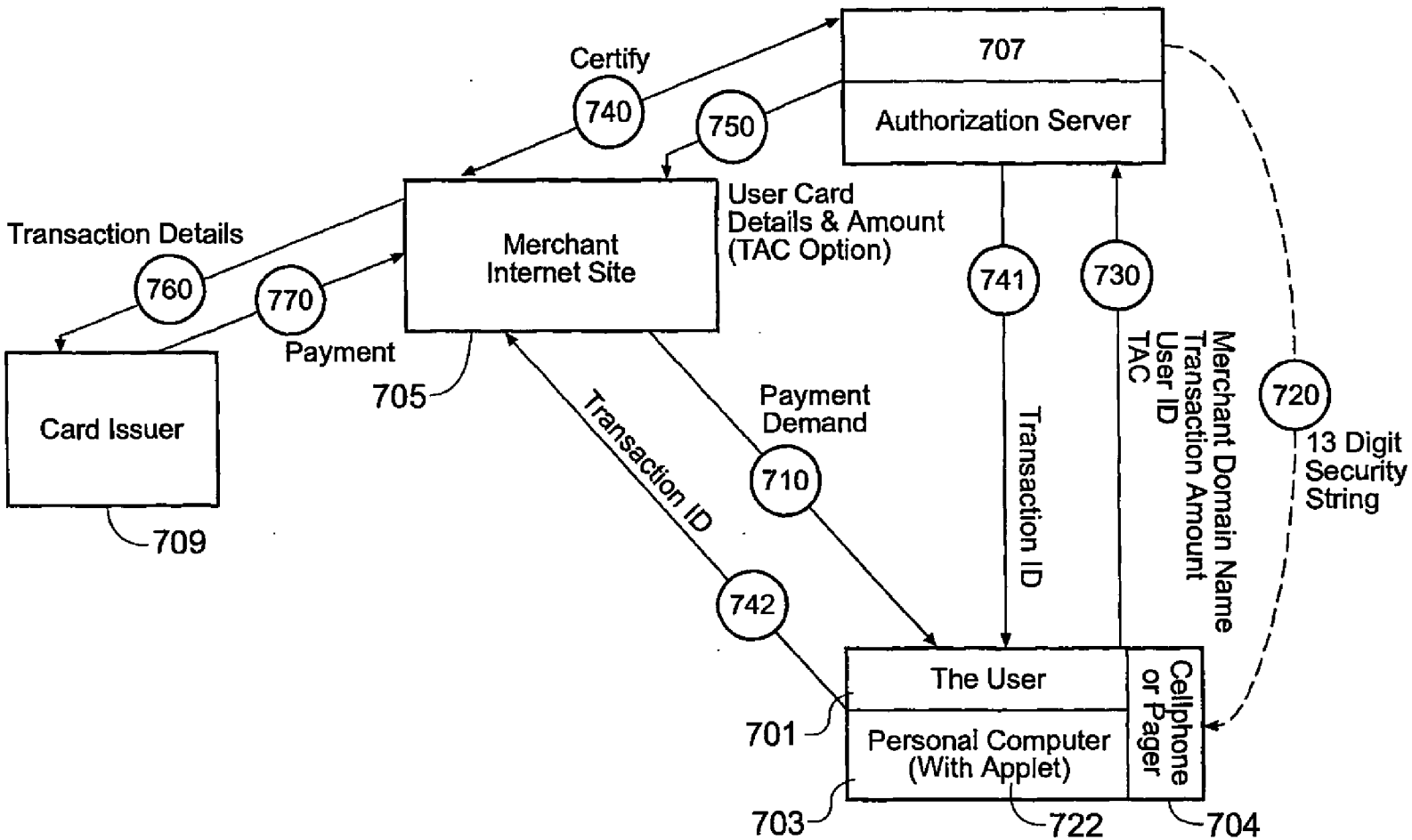
707
Authorization Server
Certify
740
750
Merchant Internet Site
User Card Details & Amount (TAC Option)
Transaction Details
760
770
Payment
705
Card Issuer
709
Payment Demand
710
Transaction ID
742
741
730
Transaction ID
Merchant Domain Name
Transaction Amount
User ID
TAC
720
13 Digit Security String
The User
Personal Computer (With Applet)
Cellphone or Pager
701
703
722
704

Fig. 7

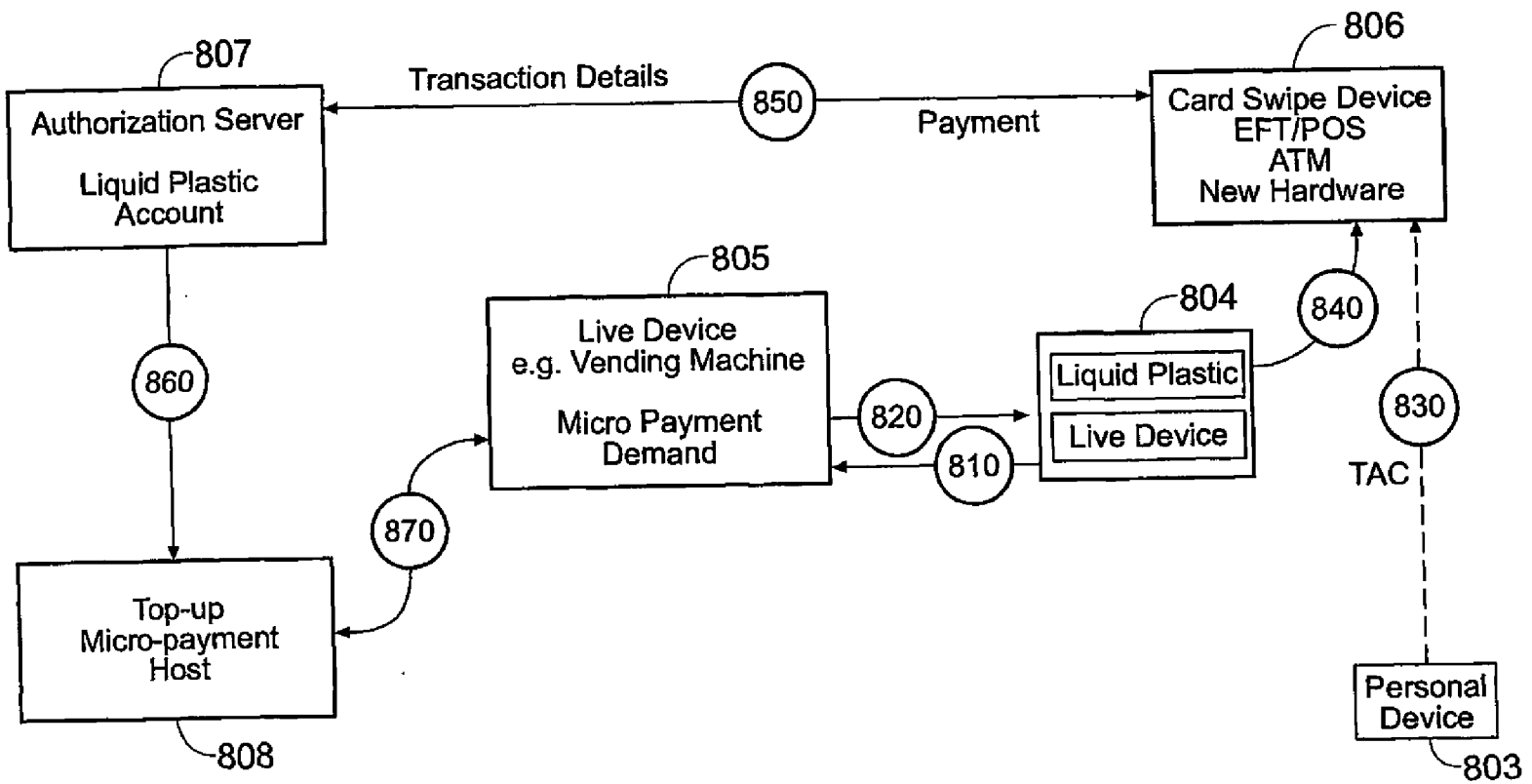
807
Authorization Server
Liquid Plastic Account
Transaction Details
850
Payment
806
Card Swipe Device
EFT/POS
ATM
New Hardware
805
Live Device
e.g. Vending Machine
Micro Payment Demand
804
Liquid Plastic
Live Device
840
820
810
860
870
830
TAC
Top-up
Micro-payment
Host
808
Personal Device
803

Fig. 8

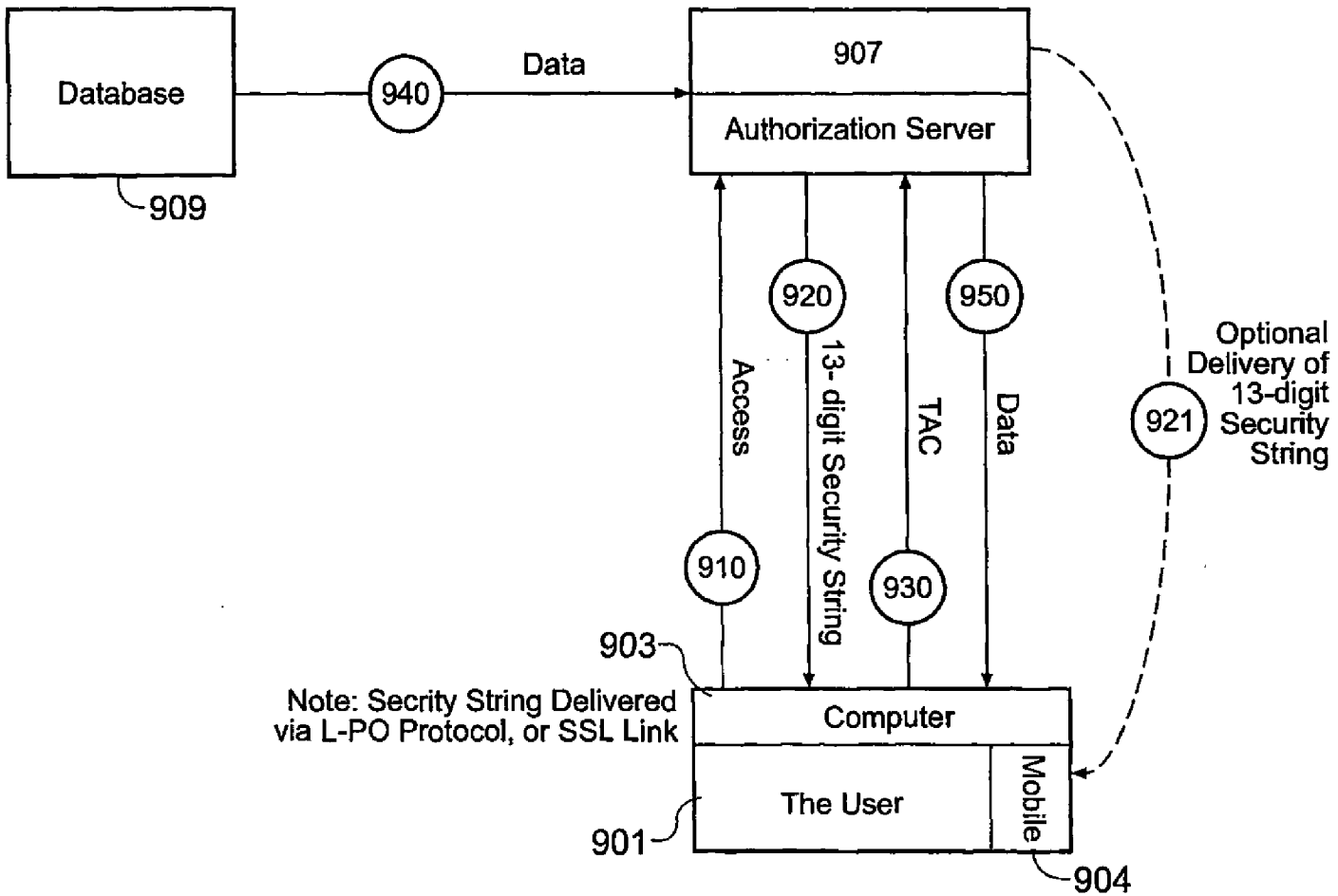
Database
909
940
Data
907
Authorization Server
920
950
Access
13- digit Security String
TAC
Data
Optional Delivery of 13-digit Security String
921
910
930
903
Note: Secrity String Delivered via L-PO Protocol, or SSL Link
Computer
The User
Mobile
901
904

Fig. 9

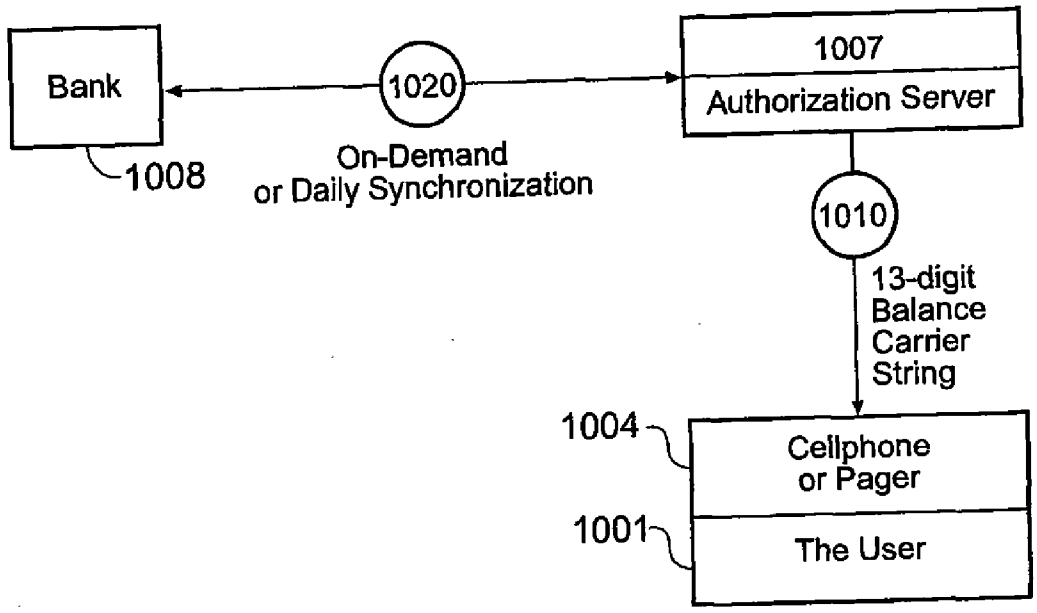

Fig. 10

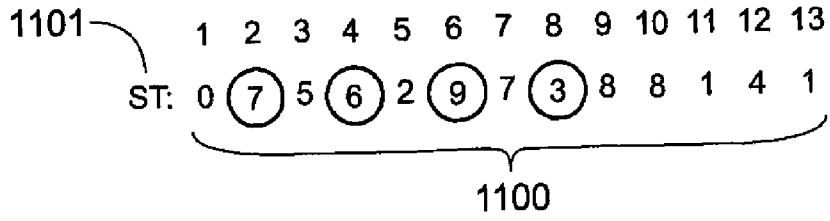

Fig. 11

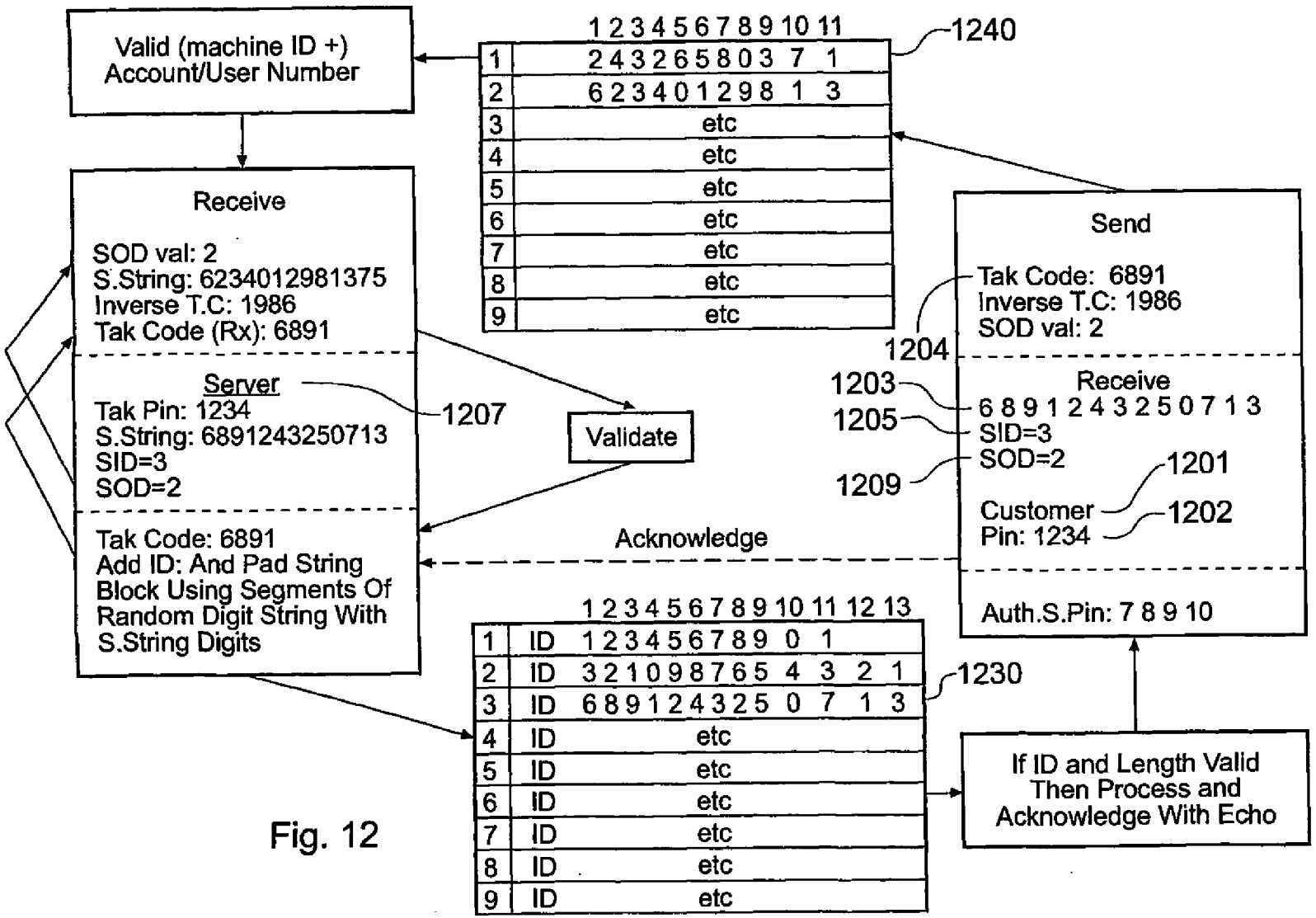
Valid (machine ID +)
Account/User Number
1 2 3 4 5 6 7 8 9 10 11
1240
1 2 4 3 2 6 5 8 0 3 7 1
6 2 3 4 0 1 2 9 8 1 3
etc
Receive
SOD val: 2
S.String: 6234012981375
Inverse T.C: 1986
Tak Code (Rx): 6891
Server
Tak Pin: 1234
S.String: 6891243250713
SID=3
SOD=2
1207
Validate
Tak Code: 6891
Add ID: And Pad String
Block Using Segments Of
Random Digit String With
S.String Digits
Send
Tak Code: 6891
Inverse T.C: 1986
SOD val: 2
1204
1203
1205
1209
Receive
6 8 9 1 2 4 3 2 5 0 7 1 3
SID=3
SOD=2
1201
Customer
1202
Pin: 1234
Acknowledge
Auth.S.Pin: 7 8 9 10
1 2 3 4 5 6 7 8 9 10 11 12 13
1230
ID 1 2 3 4 5 6 7 8 9 0 1
ID 3 2 1 0 9 8 7 6 5 4 3 2 1
ID 6 8 9 1 2 4 3 2 5 0 7 1 3
ID
If ID and Length Valid
Then Process and
Acknowledge With Echo

Fig. 12

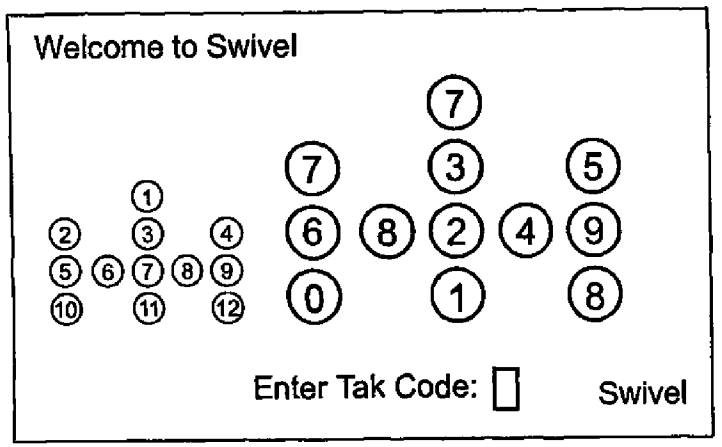

Fig. 13a

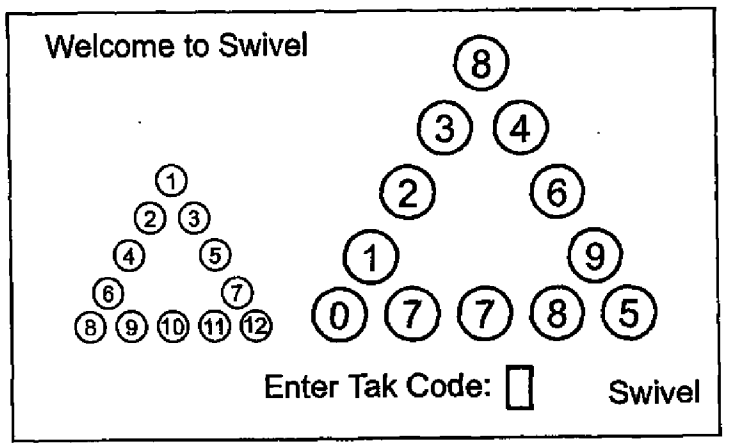

Fig. 13b

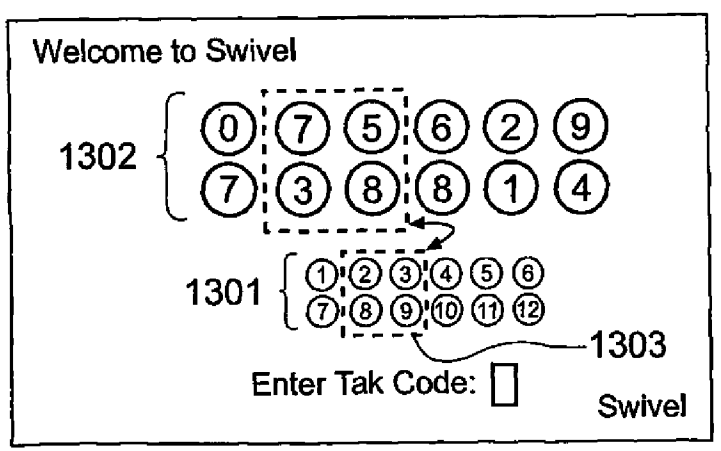

Fig. 13c

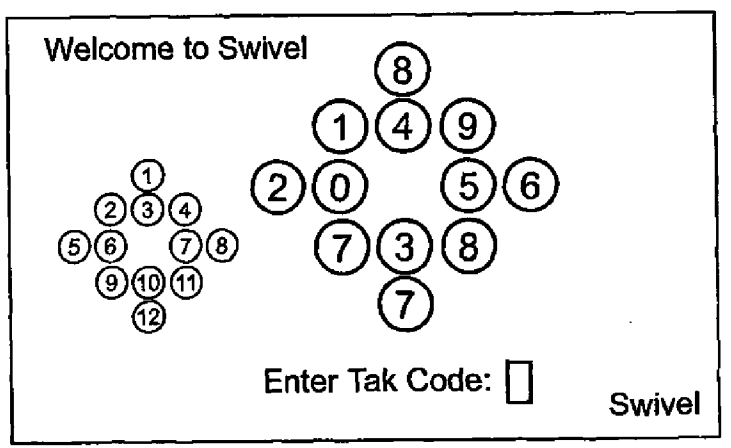

Fig. 13d

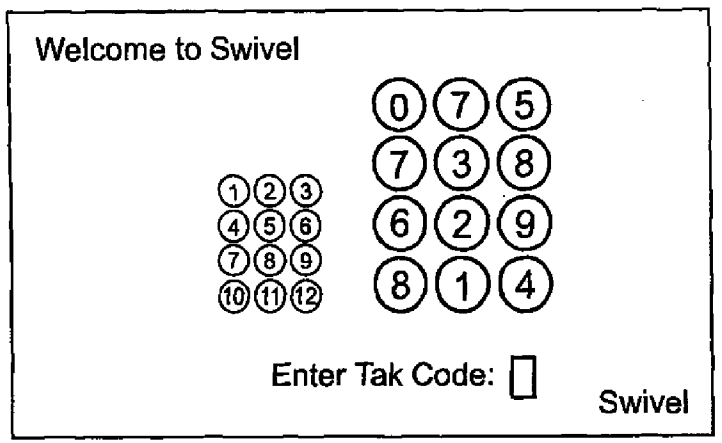

Fig. 13e

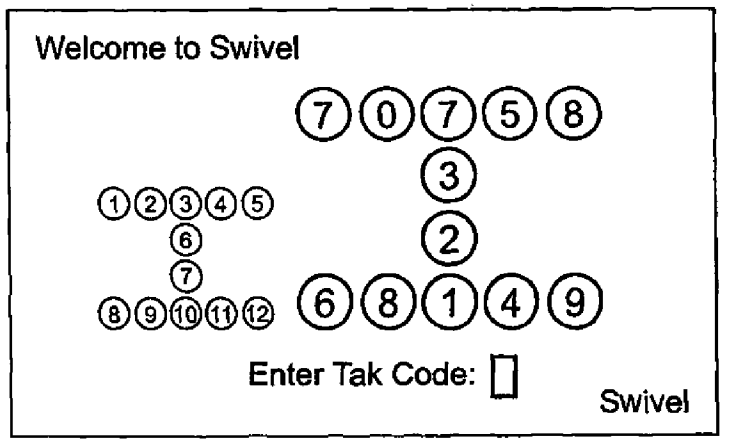

Fig. 13f

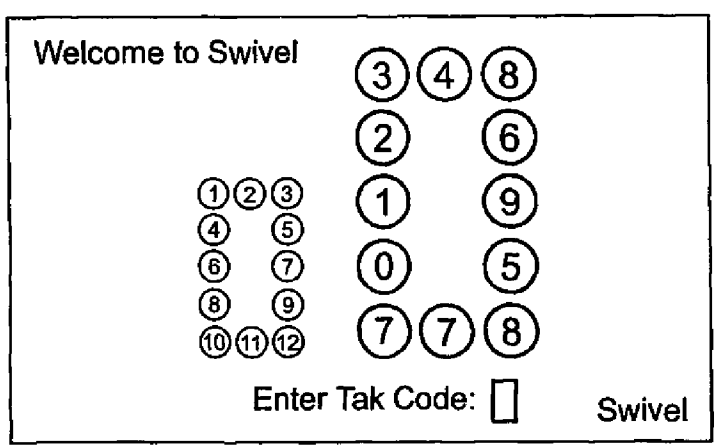

Fig. 13g

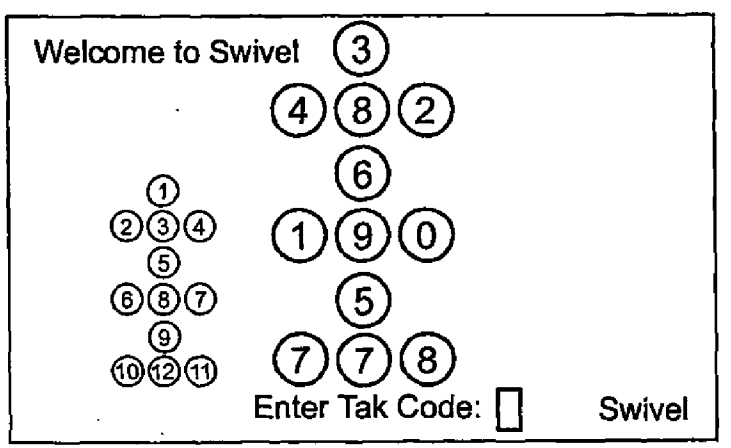

Fig. 13h

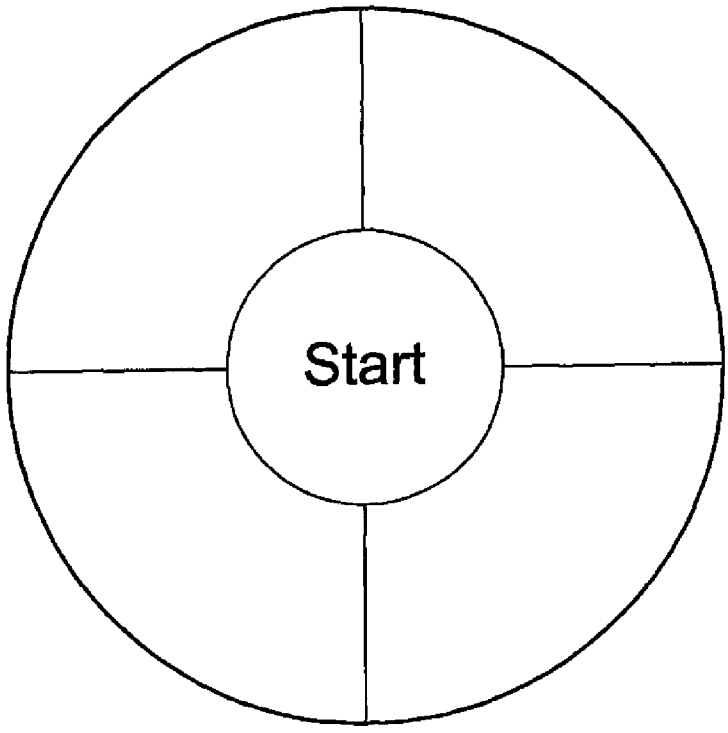

Fig. 14

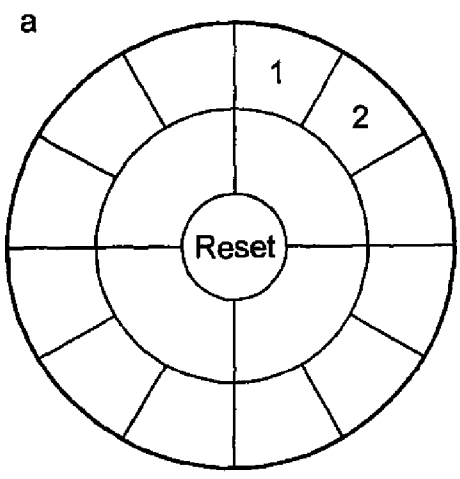

Fig. 15a

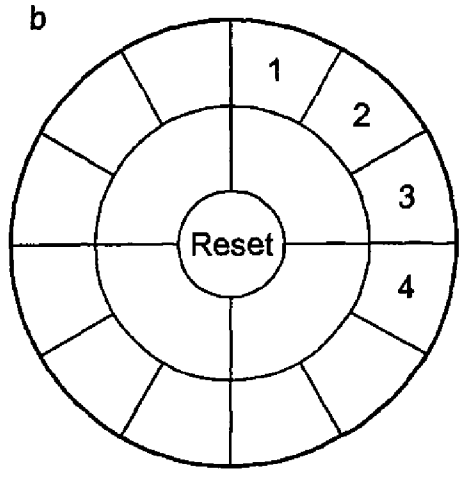

Fig. 15b

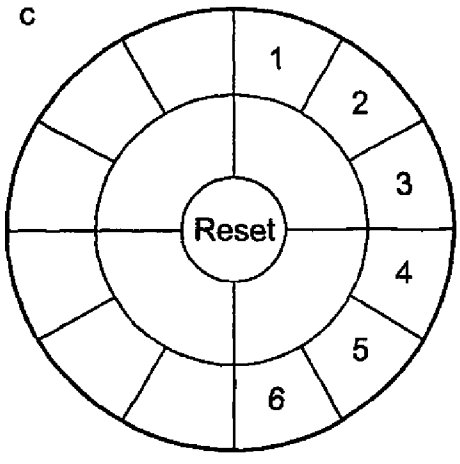

Fig. 15c

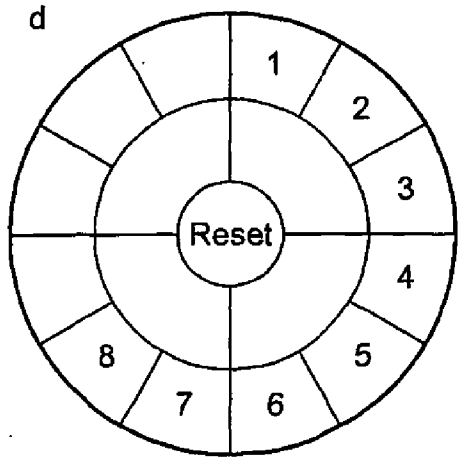

Fig. 15d

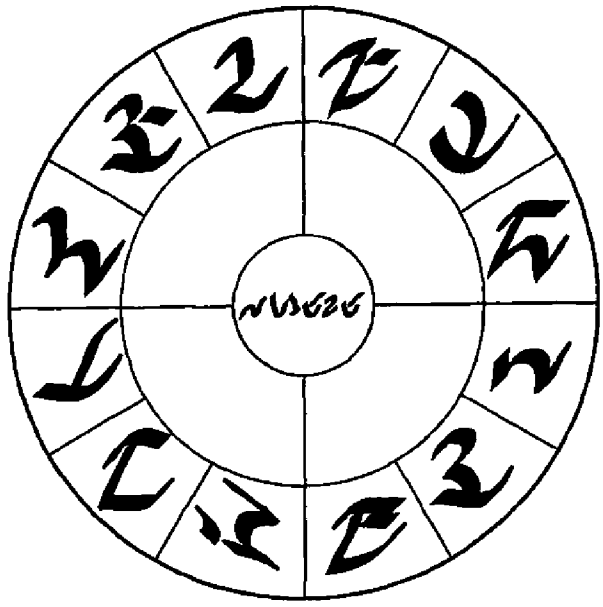

Fig. 15e

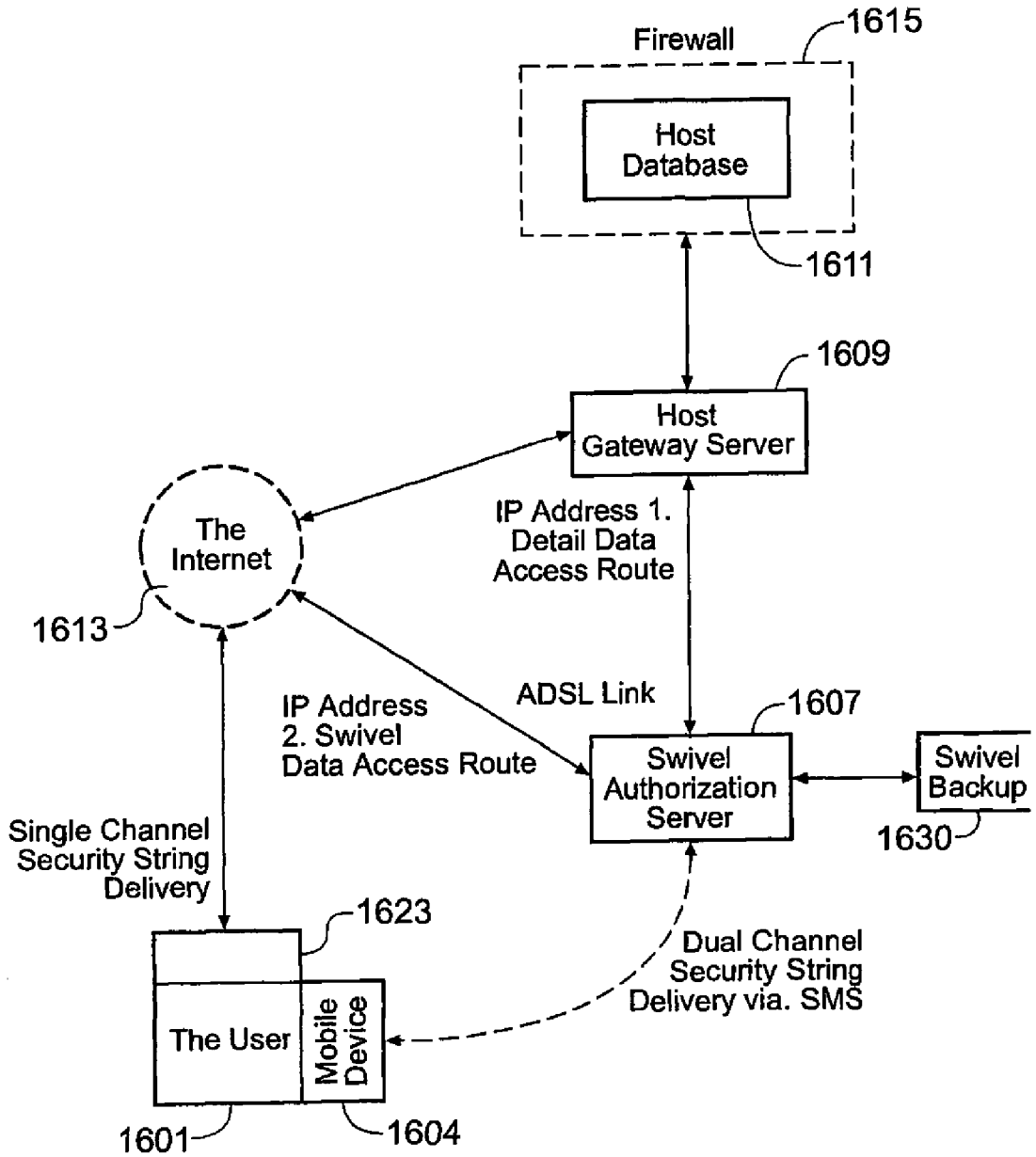

Fig. 16

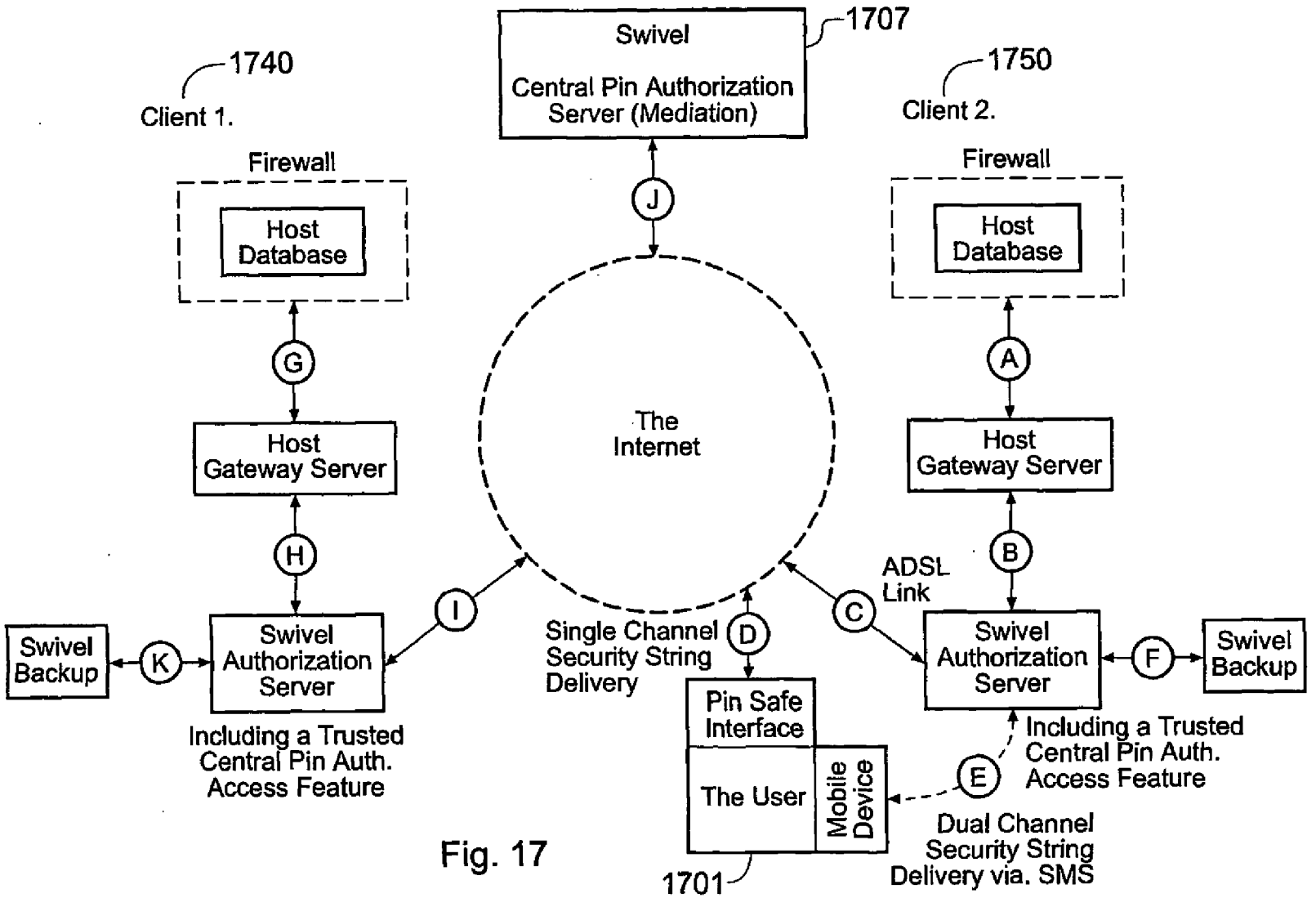
Swivel
Central Pin Authorization Server (Mediation)
1707
1740
Client 1.
1750
Client 2.
Firewall
Host Database
Firewall
Host Database
J
G
A
The Internet
Host Gateway Server
Host Gateway Server
H
B
ADSL Link
I
C
Swivel Backup
K
Swivel Authorization Server
Single Channel Security String Delivery
D
Swivel Authorization Server
F
Swivel Backup
Pin Safe Interface
Including a Trusted Central Pin Auth. Access Feature
The User
Mobile Device
E
Including a Trusted Central Pin Auth. Access Feature
Dual Channel Security String Delivery via. SMS
1701

Fig. 17

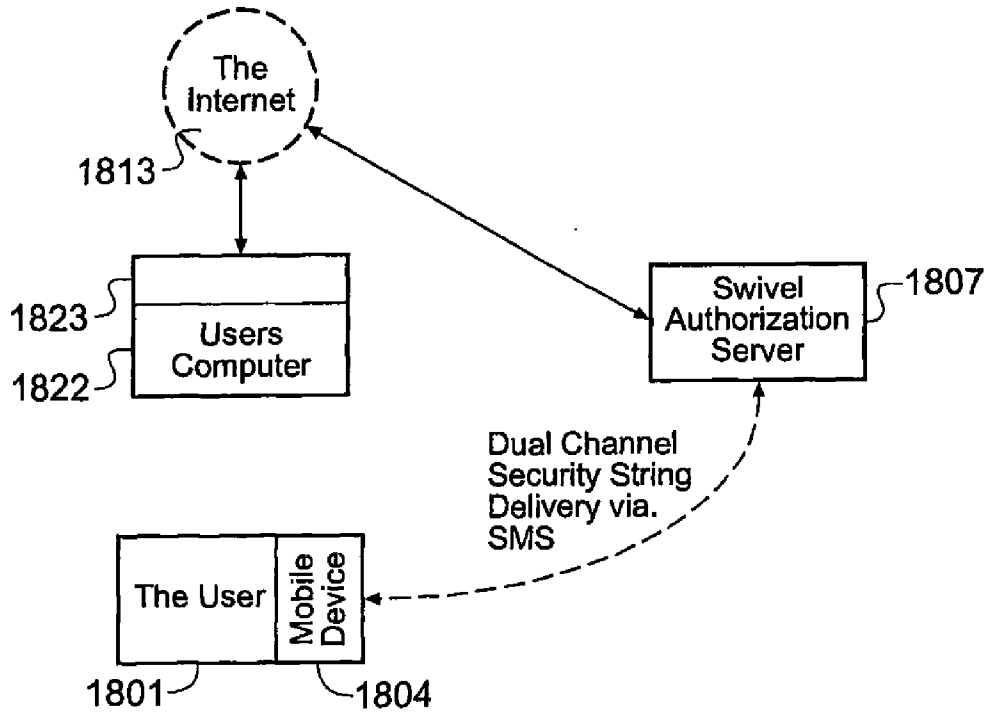

Fig. 18

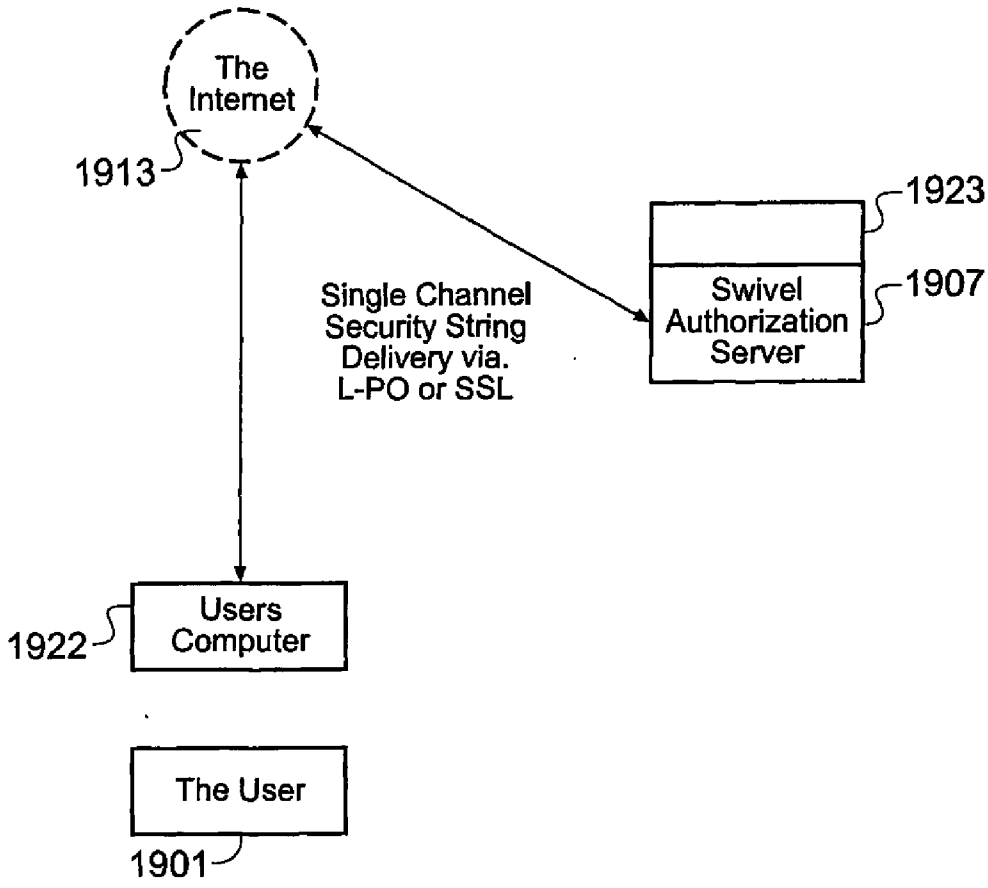

Fig. 19

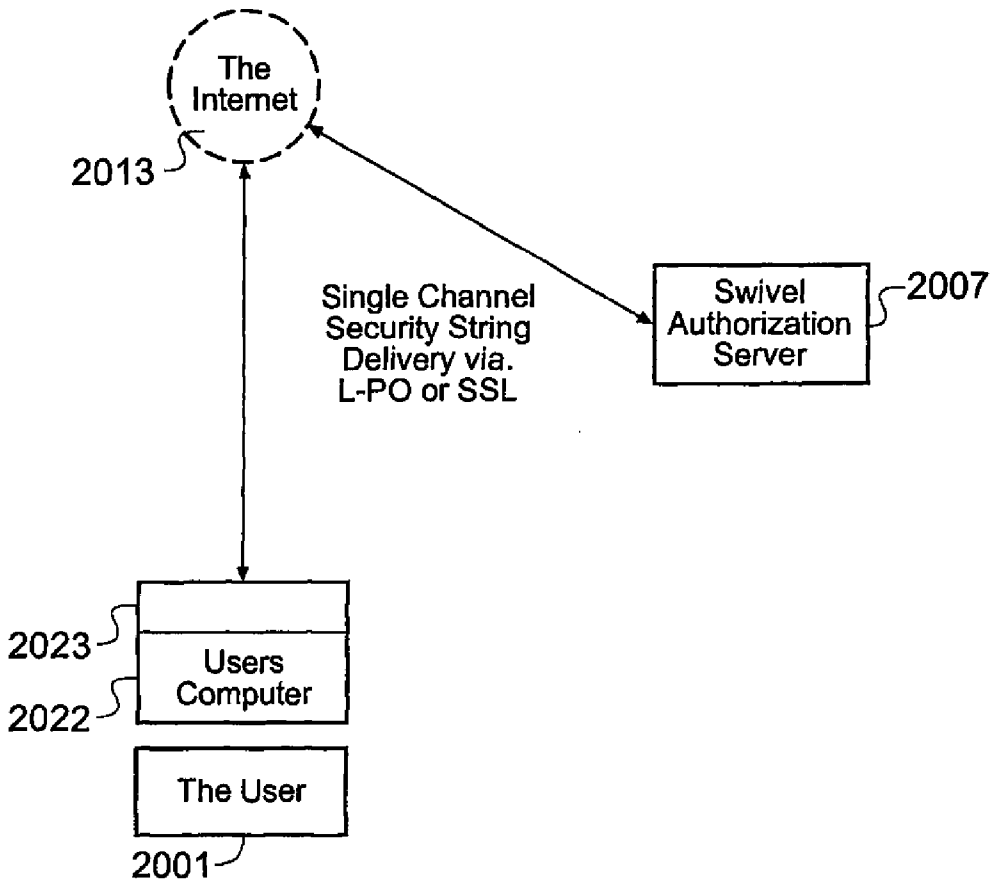

Fig. 20

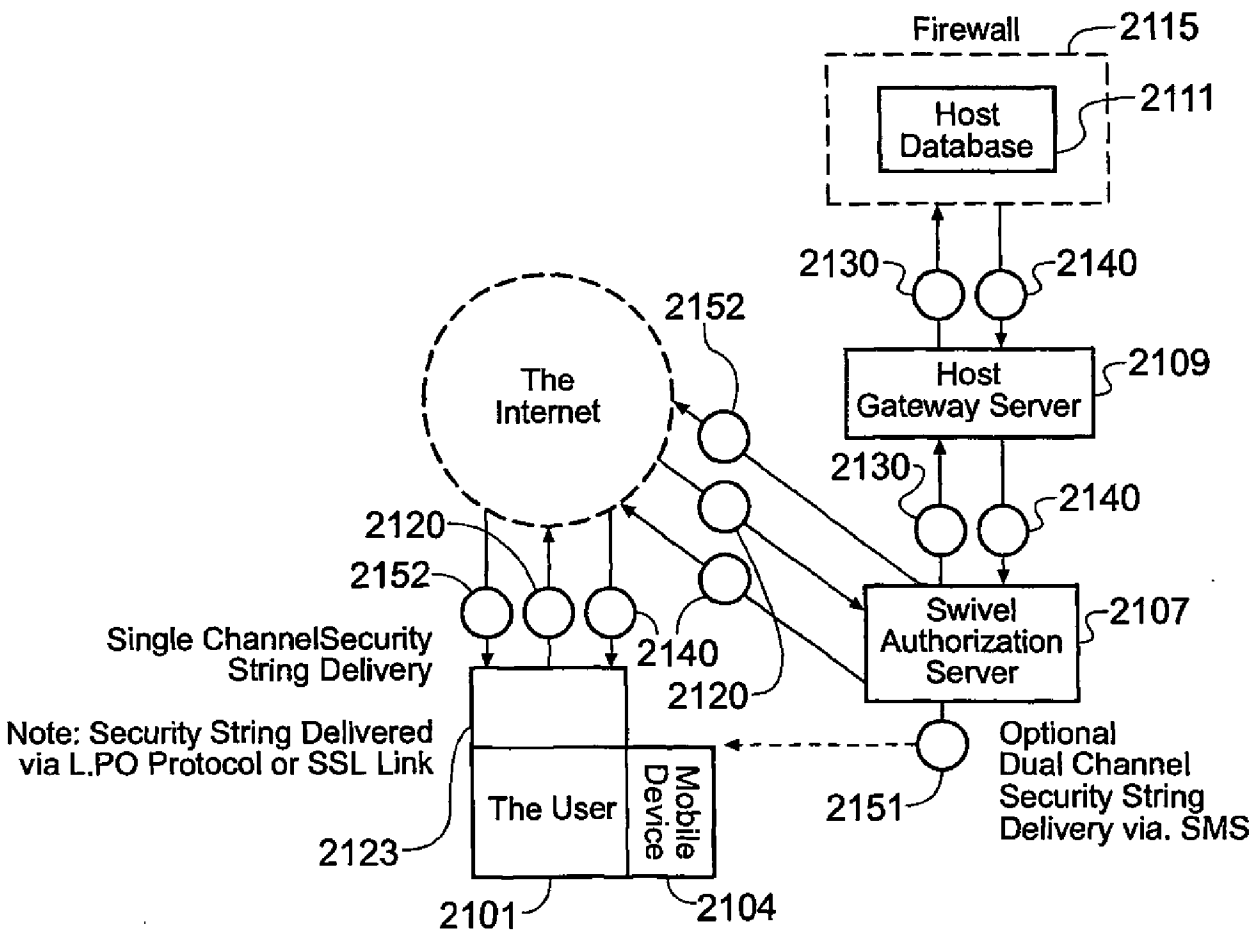
Firewall
2115
Host Database
2111
2130
2140
2152
The Internet
Host Gateway Server
2109
2130
2140
2120
2152
Swivel Authorization Server
2107
Single ChannelSecurity String Delivery
2140
2120
Note: Security String Delivered via L.PO Protocol or SSL Link
Optional Dual Channel Security String Delivery via. SMS
2151
The User
Mobile Device
2123
2101
2104

Fig. 21

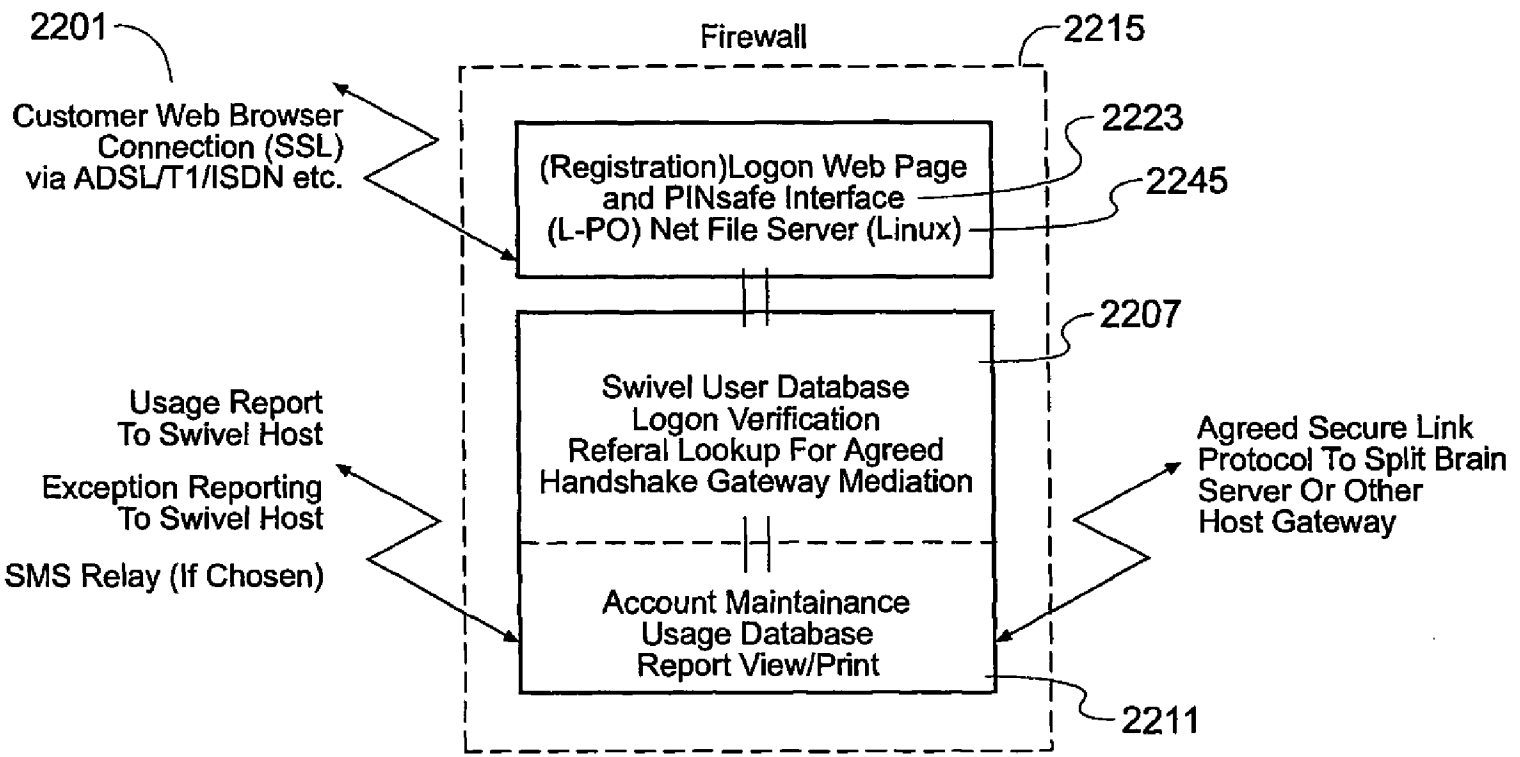
2201
Customer Web Browser
Connection (SSL)
via ADSL/T1/ISDN etc.
Firewall
2215
(Registration)Logon Web Page
and PINsafe Interface
(L-PO) Net File Server (Linux)
2223
2245
2207
Swivel User Database
Logon Verification
Referal Lookup For Agreed
Handshake Gateway Mediation
Usage Report
To Swivel Host
Exception Reporting
To Swivel Host
SMS Relay (If Chosen)
Account Maintainance
Usage Database
Report View/Print
2211
Agreed Secure Link
Protocol To Split Brain
Server Or Other
Host Gateway

Fig. 22

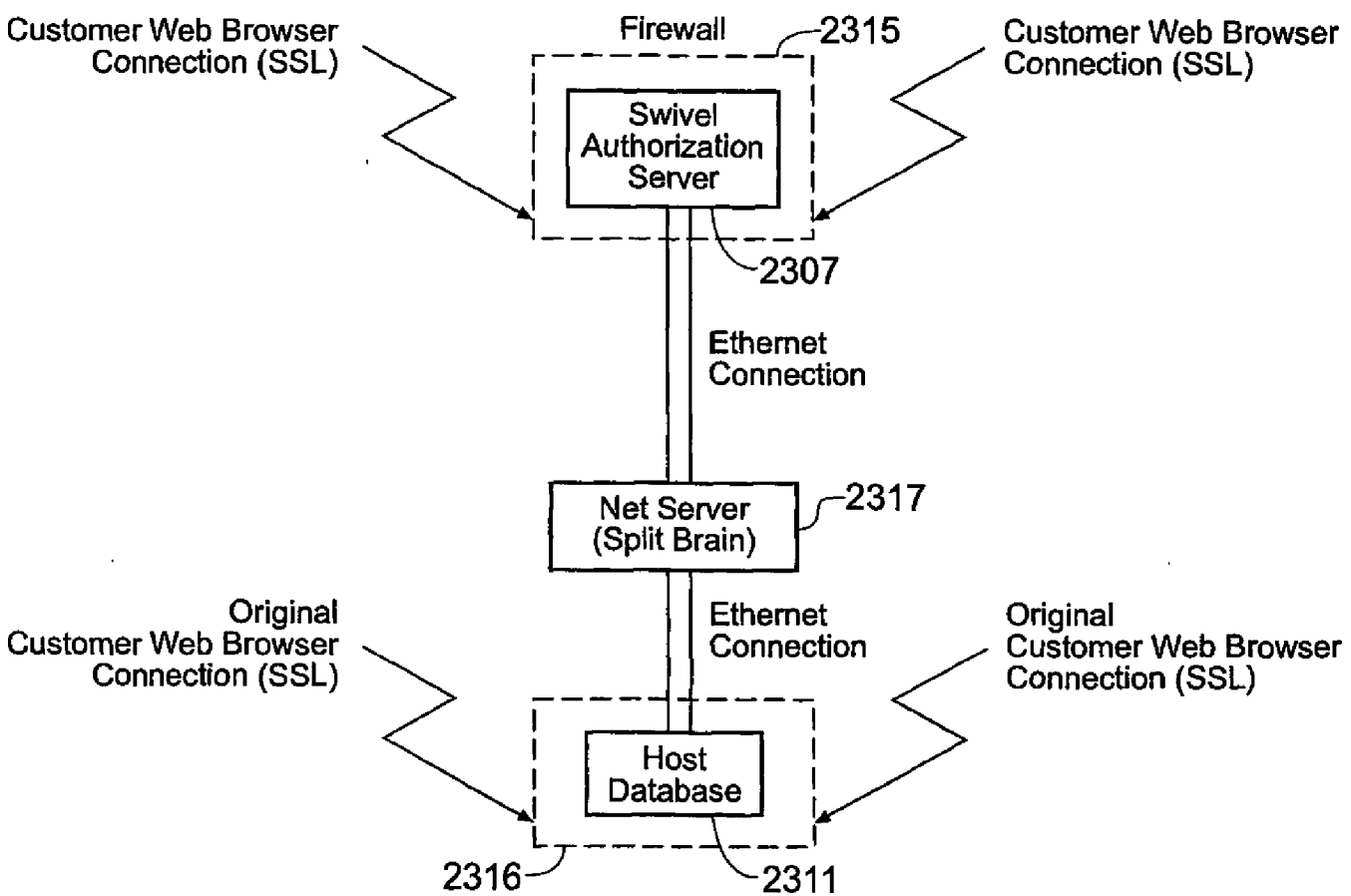
Customer Web Browser Connection (SSL)
Firewall
2315
Customer Web Browser Connection (SSL)
Swivel Authorization Server
2307
Ethernet Connection
Net Server (Split Brain)
2317
Original Customer Web Browser Connection (SSL)
Ethernet Connection
Original Customer Web Browser Connection (SSL)
Host Database
2316
2311

Fig. 23