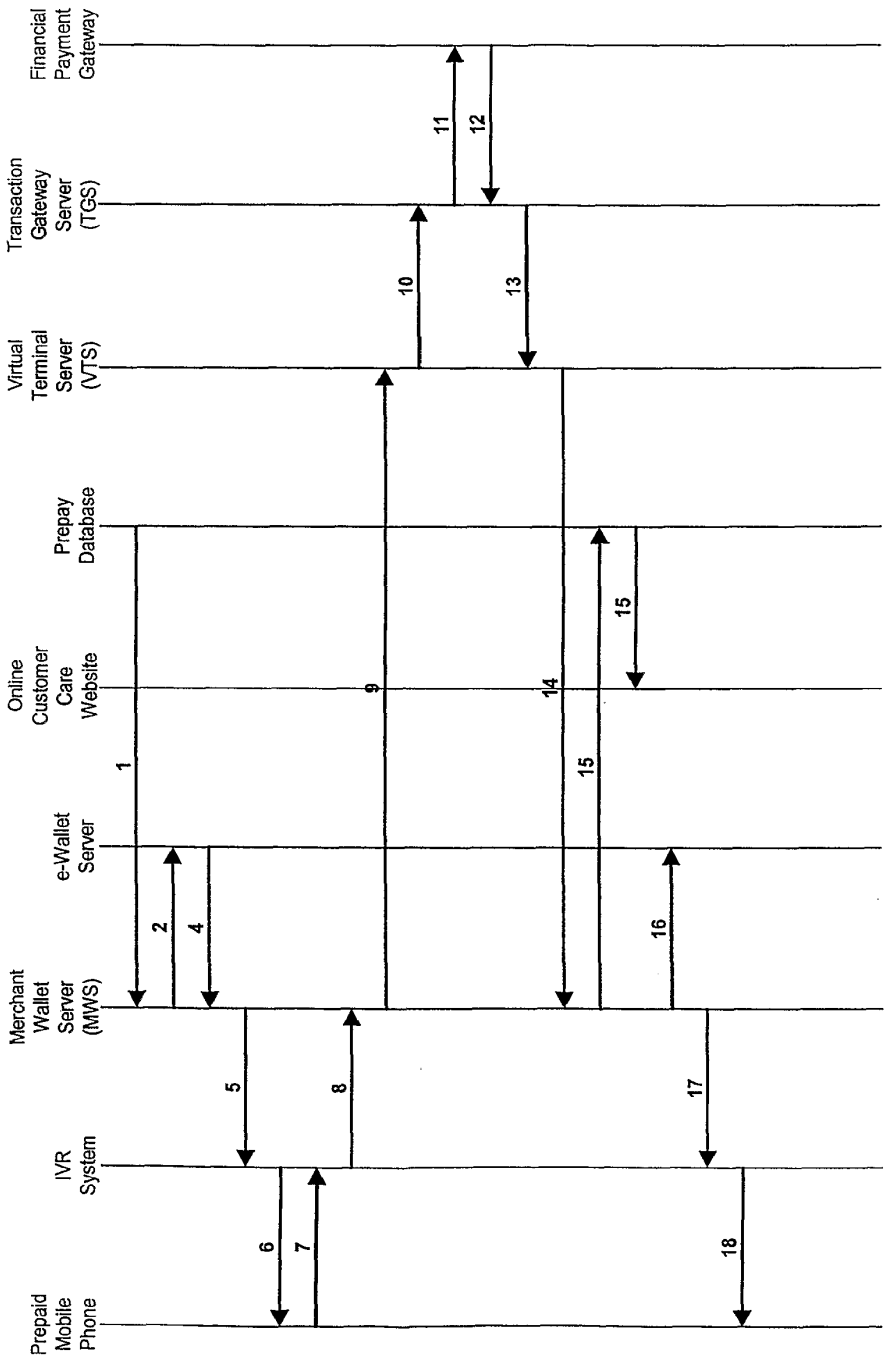

Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
IVR System
Prepaid Mobile Phone
1
2
4
5
6
7
8
9
10
11
12
13
14
15
15
16
17
18

Figure 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 February 2003 (13.02.2003)

PCT

(10) International Publication Number
WO 03/012717 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/23899

(22) International Filing Date: 30 July 2001 (30.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: C-SAM, INC. [US/US]; Suite 2060, One Tower Lane, Oakbrook Terrace, IL 60181 (US).

(72) Inventor: PITRODA, Satyan, G.; Suite 2060, One Tower Lane, Oakbrook Terrace, IL 60181 (US).

(74) Agent: SHEKLETON, Gerald, T.; Welsh & Katz, Ltd., 120 S. Riverside Plaza, 22nd Floor, Chicago, IL 60606 (US).

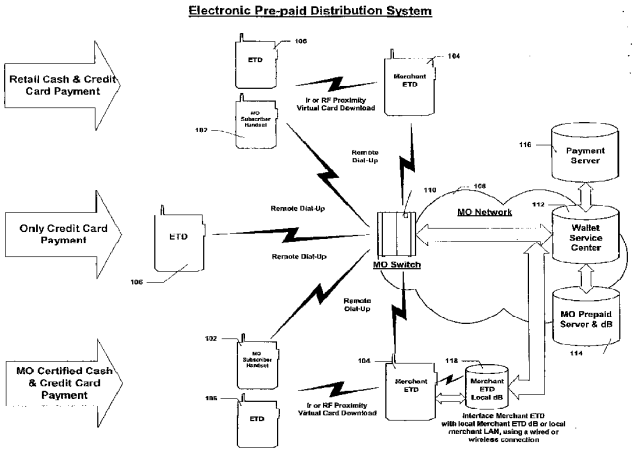
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR DISTRIBUTION AND USE OF VIRTUAL STORED VALUE CARDS



(57) Abstract: A method of exchanging payment information in an electronic transaction includes a first electronic transaction device (106) transferring payment information to a second electronic transaction device (106), the second electronic transaction device (104) transferring value information to the first electronic transaction device (106), and the second electronic transaction device (104) transferring value information and payment information to a service consolidation centre (112). A method of tracking retail sales of pre-paid telephone cards to cash subscribers is also provided. This method comprises entering value purchased information and subscriber information in a retailer electronic transaction device (104), the retailer electronic transaction device (104) transferring the value purchased information and subscriber information to a mobile operator (102), and the mobile operator (102) adding value corresponding to the value purchased information to an account corresponding to the subscriber information.

WO 03/012717 A1

SYSTEM FOR DISTRIBUTION AND USE OF VIRTUAL STORED VALUE CARDS

BACKGROUND OF THE INVENTION

This invention relates to a new and improved system for distribution and use of virtual stored value cards. One particular example where the invention may be used is in pre-paid virtual cards for mobile voice and data services.

Wireless or mobile phone operators typically have post-pay and pre-paid subscribers for their voice & data services. Post-pay subscribers pay for airtime they use at the end of a billing period, typically at a pre-determined rate, once a month. Pre-paid subscribers, in contrast pay for a pre-set amount of airtime, at a pre-determined rate, before they start using the airtime purchased. Pre-paid subscribers essentially create a stored-value account, from which they can use the minutes that they have purchased. The mobile operator's system keeps track of the minutes purchased and subsequently used by pre-paid subscribers and prompts them as their stored-value amounts near depletion. At this point pre-paid subscribers have the option to replenish their airtime. The operation of adding more minutes of airtime to an existing pre-paid account is typically referred to as the "top-up" or "top-off" operation.

Pre-paid services are one of the fastest growing segments of the mobile telephone operator business (mobile operators or MO). Pre-paid customers require no credit, no deposits, no contracts, no account fee, no age limit, but simply a periodic top up. Pre-paid customers do not need to demonstrate established credit or provide any details to mobile operators.

As the cost of mobile handsets and associated infrastructure has steadily decreased over time, many markets have seen an exponential increase in mobile users. As the current trend continues, the number of mobile installations may outgrow existing landlines. As the mobile handsets improve (hardware - processing power and memory, software, display – size and resolution, form factor, battery life, etc.) and the bandwidth offered by the mobile operator's increase, the new services offered by mobile operators will increase substantially. Because of decreasing costs of the handsets and the potential of value added services, mobile operators have been able to subsidize handset costs and offer pre-paid services to a large number of new customers to increase market share substantially. In some markets pre-paid customers account for as much as 70 to 80% of the total customer base. The pre-paid services have become popular for several reasons.

Pre-paid subscribers do not have to deal with long-term contracts – an element typical to a lot of calling plans offered by mobile operators to essentially allow them to subsidize the cost of the mobile handset. As the cost of handsets has continued to drop, and also as handset churn rates continue to climb, subscribers have the opportunity of purchasing second hand devices, further increasing the number of overall wireless subscribers. Owing to these factors, the mobile operators can now afford to offer pre-paid calling plans without any rigorous long-term contracts.

Since pre-paid calling plans do not require the subscriber to pay the charges at the end of the billing cycle, cash starved subscribers do not have to set aside any funds. This allows the subscriber to purchase service, without any elaborate budgeting.

Pre-paid subscribers do not have to deal with any unused airtime on fixed plans. For instance, typical plans will have a preset number of minutes of airtime for

a certain value, which would expire at the end of the month. If these minutes are not used, they expire and the subscriber loses the value associated with the unused airtime.

Pre-paid subscribers do not require a credit account, or in many cases even a bank account, allowing them to purchase the service over the counter using cash, at various retail outlets and mobile operator certified distribution centers in the form of "scratch-off" plastic cards. This is ideal for the lower and middle income groups, students, and also for pre-dominantly cash economies, in emerging markets, where the pre-paid product has been very successful.

Mobile Operators ("MO") typically distribute their handsets (or alternately SIM cards) to pre-paid subscribers through controlled distribution channels – certified distribution outlets and/or participating retailers. The handsets come with some airtime preinstalled, as an incentive to the subscriber, and also allowing them to call the mobile operator to setup and "top-up" an account. The top-up operation to replenish airtime for pre-paid accounts may be accomplished in one of the following ways (Figure 1 and Figure 2):

The subscriber may top-up a pre-paid account by dialing into the MO's system, using their established payment account – credit, debit, etc. This may be done manually by speaking to a MO customer service representative, by using an automated voice activated response ("VAR") system, or through the Internet.

To manually top-up a pre-paid account, the subscriber calls an MO customer service representative, reads the pre-paid account number, and states the additional airtime required and the preferred payment method, which involves reading the credit card account number, expiry date, etc. This typically involves a dedicated session

between the subscriber and the customer service representative, which is cumbersome, labor intensive and expensive.

In contrast, the automated VAR procedure involves dialing into the MO's system, selecting the number of minutes or airtime required, and entering or setting up a payment account, typically using the MO's automated voice activated response system.

One of the channels for top-up is through the Internet. Pre-paid subscribers may top-up their accounts by connecting to the mobile operator's pre-paid system through the Internet, entering a password to access their account and top-up using a credit account.

In addition, a subscriber may setup a new pre-paid account, or alternately top-up an existing account by going to a MO certified distribution center. These distribution centers may either be a retail environment, or possibly a certified bank that allows the subscribers to top-up their accounts using their ATM infrastructure or bank checks.

One of the more popular methods of top-up, especially for people who do not have a credit card or bank account or established credit and want to use just cash, requires purchasing a plastic card with a code for cash, which typically would be scratched off by the purchaser. These cards are distributed at the retail establishment – grocery stores, gas stations, etc. – in various denominations such as $10, $20, $50, $100, etc., where the subscriber would purchase a plastic card for the amount of required airtime. This plastic card is distributed in a tamper proof package, and is purchased from a retailer. The subscriber then scratches off the code, enters this code manually through the mobile handset into the MO's system, which in turn replenishes the amount of airtime purchased by the subscriber.

There are several disadvantages to present methods of topping-off pre-paid accounts. The mobile operators' cost for offering pre-paid airtime is as high as 20-30%. These costs are essentially incurred at various levels, for printing, packaging and distributing the cards, commissions for various intermediaries, depending on the distribution channel and process adopted. The manual system incurs additional labor costs, since it requires a dedicated customer service representative to walk the subscriber through the entire setup and top-up process. Add to this, the credit card issuer's fees for the transaction ("Card Holder Not Present" (CHNP) transactions), and the overall cost incurred by the mobile operator to support this distribution channel is very high.

The automated VAR channel may reduce a fraction of the cost by removing the labor component from the manual system. But this process has proven to be extremely cumbersome. Topping-up the account from the mobile device handset is awkward for the user, given the state of the handset's form factor, user interface, screen and keypad sizes. Thus, errors occur, especially during the setup operation, when the user must alternatively hold the handset near the ear to hear the VAR system and then hold it in front of the eyes to dial appropriate numbers. This eventually drives impatient subscribers to less cumbersome distribution channels, which in turn have a higher cost associated to the model for the mobile operator.

Certified MO distributors typically provide over-the-counter service for pre-paid subscribers, which incurs retail costs, in addition to the costs mention above. Because there are only a limited number of certified centers, the overall reach of such distribution centers is limited. Since many of these certified centers have a direct hook-up into the MO's back-end system, adding on such centers require more direct

hook-ups, increasing the potential of fraud and adds to the accounting and inventory management costs.

Neutral distributors who support several mobile operators' products, typically charge a high margin for shelf space, increasing the distribution cost for the mobile operator.

One of the most popular channels of distribution for pre-paid products is through existing retail distribution channels - gas stations, grocery and department stores, etc. The reach of these channels, along with the ability to use cash, are the top most reasons for its popularity, but are also the most expensive for the mobile operator to support.

The mobile operator incurs some cost for producing the plastic cards, packaging and distributing them. In addition, the mobile operator incurs costs for tracking and managing physical inventory, ironically for a non-physical or virtual product such as airtime.

Retailers charge the mobile operators a very high margin for the distribution of these plastic cards, as they take up expensive shelf space. These margins form one of the integral components of the overall costs incurred by the mobile operator for the distribution of plastic pre-paid cards. Cash handling expenses, and credit card fees add to the overall cost, along with other cost elements typical to a retail environment.

Regarding transactions in general, the cost of a transaction, in the existing credit or debit environments supported by the widely accepted banking networks, typically ranges between 1.2 to 5.0% of the transaction, plus an additional 10 to 35 cents. The cost these transactions renders existing credit and debit transaction systems impractical for "sub to single digit dollar" transactions, typically referred to as micro-payments. Many transactions, especially proximity transactions for applications such

as vending machines, toll, parking and transit, fall under this category which could be well supported by a stored cash value payment system.

The current stored value payment systems are inefficient, due to the lack of interoperability across payment worlds and end to end security. Consequently, the existing stored value payment systems have not been able to successfully cater to the eCommerce and mCommerce environments. In the brick and mortar retail environment, again the lack of a truly global interoperable and secure system has been responsible for less acceptance by merchants and consequently less penetration among users. The existing systems have also failed to provide an effective payment system for minors, who typically do not qualify for a credit or debit card, for credit challenged individuals and for person to person transactions.

Because existing credit and debit transaction systems are impractical for micropayments, cash is the predominant form of payment. Cash may be cumbersome, subject to theft or loss, and in some cases owing to the lack of local currency, impractical and extremely inconvenient. In terms of the merchants, owing to the high potential of fraud and theft, cash transactions are associated with a very high cost of handling and collection. Thus need exists for a suitable payment system to address the above outlined issues, and at the same time reduce cash transactions for the convenience of the users and merchants alike.

DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram of a prior-art pre-paid distribution system.

Figure 2 is a flow chart of a prior art pre-paid distribution system.

Figure 3 is a diagram depicting a preferred embodiments of the electronic pre-paid distribution system of the present invention.

Figure 4 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment of the present invention.

Figure 5 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment Through MO Network of the present invention.

Figure 6 is a diagram depicting a preferred embodiment of the Retail & MO Certified Cash & Credit Card Payment Through Proximity of the present invention.

Figure 7 is a diagram depicting a preferred embodiment of the Only Credit Card Payment of the present invention.

Figure 8 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Setup Sequence Flow Chart of the present invention.

Figure 9 is a diagram depicting a preferred embodiment of the Only Credit Card Payment "Top-Off" Sequence Flow Chart of the present invention.

Figure 10 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Sample User Interfaces is of the present invention.

Figure 11 is a diagram depicting a preferred embodiment of the Only Credit Card Payment Sample User Interfaces of the present invention.

Figure 12 is a diagram depicting a preferred embodiment of the Merchant Wallet Architecture of the present invention.

Figure 13 is a diagram depicting a preferred embodiment of the Merchant Wallet Sample User Interfaces is of the present invention.

Figure 14 is a diagram depicting a preferred embodiment of the Wallet Service Center Value Added Services of the present invention.

Figure 15 is a diagram of examples of virtual card generation and download.

Figure 16 is a diagram of a stored value application of the present invention.

Figure 17 is a diagram of a preferred embodiment of a stored value transaction system Through MO Network of the present invention.

Figure 18 is a flow chart of a preferred embodiment of a stored value transaction system Through MO Network of the present invention.

Figure 19 is a diagram of a stored value transaction system proximity model of the present invention.

Figure 20 is a flow chart of a preferred embodiment of a stored value transaction system of the present invention.

Figure 21 is a diagram of a multiple MO example of the present invention.

Figure 22 is a diagram of examples of user interfaces for a multiple MO environment of the present invention.

Figure 23 is a diagram of an Existing Transaction System and a Wireless Transaction System.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

For purposes of reference, Figures 1 and 2 are diagrams that generally depict various aspects of prior art distribution of pre-paid air time. Figure 1 shows existing channels of distribution for pre-paid airtime, the setup and top-up operations using a mobile handset and the mobile operator's manual or automated systems, using the mobile operator certified locations and the retail outlet model to procure plastic pre-paid "scratch-off cards."

Figure 2 is a flowchart depicting current distribution processes for a mobile handset with pre-paid airtime.

As shown in Figure 1, MO Network 20 includes MO Switch 22 and MO Pre-paid Server and Database 24. MO Certified Distribution Center 26 is coupled to the MO Pre-paid Server and Database 24. MO Subscriber Handset 28 is in electronic

communication with MO Switch 22. Pre-paid Plastic Card Retail Distribution Centers 30 are not connected to the MO Network 20. MO Subscribers may connect to the MO Network 20 by way of a Computer 32 connected to the Internet 34.

Figure 3 illustrates examples of the pre-paid distribution systems of the present invention. A MO Subscriber Handset 102 may be topped up by way of an electronic transaction device (ETD) adapted to the functions of a Merchant (hereinafter Merchant ETD 104). Electronic transaction devices include, but are not limited to, devices such as the Universal Electronic Transaction Card as disclosed in U.S. Patent Nos. 5,590,038 and 5,884,271, which are incorporated by reference. To facilitate the transaction. the MO Subscriber may also have a MO Subscriber ETD 106 adapted to communicate with the Merchant ETD 104. The MO Subscriber ETD 106. It may be a separate device as illustrated, or it may be embedded in the MO Subscriber Handset 102. Alternatively, the subscriber may communicate with Merchant ETD 104 as illustrated in Figures 12, 13, and 14. The Merchant ETD 104 is in electronic communication with MO Network 108. MO network 108 includes MO Switch 110, Wallet Service Centers 112, MO Pre-paid Server 114, and Payment Server 116.

Figure 3 illustrates three examples of the invention. The first example, which is labeled "Retail Cash & Credit Card Payment," permits the MO, using a Merchant ETD 104, to distribute pre-paid airtime by taking cash or credit cards, debit cards, etc. from their customers. This typically relates to retail environment –grocery stores, gas stations, department stores, etc. - where a merchant using the Merchant ETD 104 may distribute pre-paid airtime using the MOs network or a proximity method.

The merchant enters relevant information into the Merchant ETD 104, such as value purchased information and subscriber information. Value purchased

information includes, for example, the quantity of airtime purchased, the quantity of funds transferred, mode of payment (*i.e.*, cash, credit, or other form of payment), authorization information, or other like information. Subscriber information includes, for example, an identification of a person providing a payment (including cash transactions), a telephone number for the MO subscriber handset, or other such information. Once the information is entered, the merchant transmits it in a secured manner to MO Switch 110, which, in turn transmits it to a payment consolidation center, such as Wallet Service Center ("WSC") 112 (See Figs. 4, 14). The WSC 112 authenticates the MO Subscriber Handset 102 and tops-up the MOs Pre-paid Server 114. The MO will then send a message, for example, a Short Message Service (SMS) message, to the MO Subscriber Handset 102 updating the available airtime. This method may be used with existing generation mobile handsets.

The Retail Cash & Credit Card Payment example also illustrates an example involving the transmission of a "virtual card" to the distribution outlets and, subsequently, to MO Subscriber Handsets 102. The MO distributes virtual pre-paid cards to distribution outlets, using the Wallet Service Center 112 and Merchant ETDs 104 at the respective distribution centers. The virtual cards may be distributed wirelessly and securely. The distribution outlet may use the Merchant ETD 104, upon payment for airtime, to directly "beam" into the MO Subscriber Handset 102 a virtual pre-paid card. "Beaming" may be accomplished using infrared, such as IrDA, proximity RF, or other suitable transmission protocols and circuits. For a secure transmission of the virtual pre-paid card from the Merchant ETD 104 to the MO Subscriber Handset 102, an electronic transaction device application may be installed on the MO Subscriber Handset 102. A MO Subscriber Handset 102 with an electronic transaction device application can also beam the payment directly into the

Merchant ETD 104, using either a stored value account, or an existing credit, debit, bank card, etc. account. The electronic transaction device application may store the transaction record, and upload the records to a custom transaction portal at the WSC 112.

The example labeled as "MO Certified Cash & Credit Card Payment" allows subscribers to replenish their pre-paid airtime using the same methods detailed above – i.e. using the MOs network or the proximity method. This example differs from the Retail Cash & Credit Card Payment in that the MO certified centers of distribution includes banks, ATM's, and other special outlets. Additionally, a Merchant ETD local database 118 is coupled to the MO Network 108. As outlined in Figure 3, these centers may also be equipped with Merchant ETDs 104. Subscribers with a regular mobile handset may top-up their pre-paid accounts using the MO network, and those with the electronic transaction device application installed may use the proximity method to top-up their pre-paid account. The Merchant ETD local database 118 allows the merchant to perform batch transactions, and allows the merchant to compile the subscriber usage information locally.

The Merchant ETD 104 is equipped to conduct a real-time, or batch mode transaction, for both the proximity method and the method using the MO network. The Merchant ETD local database 118 may have a wired or wireless connection with the Merchant ETD 104, or may be connected to a local area network (LAN) associated with a merchant. Where the MO certified distributors have a direct interface with the MO's pre-paid server and database, the Merchant ETD 104 integrates into their existing LAN structure.

In additional embodiments, the Merchant ETD 104 may be distributed to non traditional distribution outlets, such as taxi drivers, where the backend authentication

hook-up may be wireless. The contemplated non-traditional distribution outlets would have the ability to do real-time or batch transactions.

The example labeled "Only Credit Card Payment," demonstrates the setup and top-up operations using a MO Subscriber Handset 102 having an embedded MO Subscriber ETD 106 and the MOs automated system for setup and top-up operations for pre-paid airtime. The electronic transaction device application user interface provides the MO subscriber with a user-friendly device to complete the setup and top-up operations for pre-paid airtime accounts. In one example, the electronic transaction device application may be configured to store payment information locally on the mobile handset and send payment information (credit card or debit card details, etc.) every time a transaction is conducted. This information is securely sent to the WSC, through the MO switch, and to the respective payment servers and MO pre-paid server and database. Based on this process, the transaction may be considered a "Card Holder Present Transaction." Card Holder Present Transactions typically have lower processing fees than Card Holder Not Present Transactions.

Figure 4 illustrates in more detail the Retail & MO Certified Cash & Credit Card Payment" example. The MO Subscriber Handset 102 may be configured with the electronic transaction device application (i.e., embedded MO Subscriber ETD 106). Electronic communication, such as via proximity RF (such as Bluetooth) or Infra Red (such as IrDA) is established with the Merchant ETD 104. The Merchant ETD 104 is in electronic communication, preferably wireless communication, with MO Gateway. The MO Gateway is coupled to the WSC. The WSC includes, for example, an interface and security module 122, having a MO Interface 124, a payment server interface 126, a content provider, interface 128, and a Merchant interface 130, the interface and security module 122 is coupled to a transaction portal

132. The transaction portal 132 is coupled to a added services module 134, which is coupled to a profile engine 136. The profile engine 136 interfaces with databases 138 such as a MO database 138, a Subscriber database 140, and a Merchant database 142.

Figure 5 is a process flow-chart for the pre-paid application in a retail and MO certified environment, using either cash or credit cards as the form of payment, using the mobile operator's network. In step 150, the MO Subscriber gives the Merchant ETD 104 equipped retailer cash or a credit card and a telephone number of the MO Subscriber Handset. In step 152, the Retailer enters the telephone number and desired amount of the service to purchase. Alternatively, steps 150 and 152 may be performed electronically if the MO Subscriber Handset 102 includes the electronic transaction device application. In step 154, the Merchant ETD 104 may connect to the MO switch by dialing the MO or otherwise setting up communication over available data exchange formats, such as conventional CDPD, TDMA, CDMA and GSM formats, to connect to the WSC. In step 156, the WSC authenticates the MO Subscriber and updates the MO Pre-paid Server. Additionally, the WSC updates databases for the retailer, MO Subscriber, and MO. In step 158, the MO sends confirmation to the MO Subscriber, which may be by way of SMS (Short Message Service), and in step 160 the Merchant acknowledges payment.

Figure 6 is a flow-chart, for illustrating one example pre-paid application in a retail or MO certified environment, using either cash or credit cards as the form of payment, using the proximity transmission method. In step 162, the MO distributes virtual pre-paid cards merchants. In the illustrated example, the virtual pre-paid cards are distributed by the WSC to Merchant ETD 104s wirelessly. In step 164, the MO Subscriber may purchase a Virtual Card by electronically communicating cash or credit card information from the MO Subscriber Handset 102 to the Merchant ETD.

The electronic communication may be proximity RF or Infra Red optical. In step 166, the Merchant electronically transfers the Virtual Card to the MO Subscriber's Handset. A receipt may be included with the Virtual Card transfer. In step 168, the Merchant ETD 104 sends information pertaining to the Virtual Card transaction to the MO Server by way of the WSC. In step 170, the MO updates the value in the MO subscriber's account. In step 172, the WSC updates databases such as the Merchant database, the MO database, and the MO Subscriber database. In step 174, the electronic transaction device application on the MO handset may also update the available airtime and payment records. This example requires the MO Subscriber Handset 102 to be infra red or proximity RF enabled devices (the process flow-charts in Figures 5 & 6 relate to the configuration described in Figures 3 & 4).

Figure 7 is a more detailed illustration of the "Only Credit Card Payment" example for pre-paid applications. The MO Subscriber Handset 102, including the electronic transaction device application, is in direct communication with the MO switch. The MO switch is coupled to the WSC by MO switch 110 The WSC includes, for example, interface and security module 122, coupled to the MO interface 124, payment server interface 126, Content Provider Interface 128 and Merchant Interface 130. The interface and security module 122 is coupled to transaction portal 132. The transaction portal 132 is coupled to a valve added services module 134, which is coupled to a profile engine 136. The profile engine 136 interfaces with databases such as the MO database 138, Subscriber database 140, and Merchant database 142.

Figures 8 & 9 are process flow-charts which detail the setup and top-up operations for this particular pre-paid configuration.. Referring to Figure 8, an example of steps which may be used to initialize and use a MO Subscriber Handset

102 with an electronic transaction device application is illustrated. In step 180, a first time user activates an ETD icon 180 and in step 182 enters a MO Subscriber Handset 102 personal identification number (PIN). In the illustrated example, in step 184, a sequence will halt further use of the MO Subscriber Handset 102 after three incorrect entries. This sequence may be performed off-line.

In step 186 the MO subscriber then enters a 4 digit personal identification number (PIN) into the MO Subscriber Handset. This is to "tie-up" the subscriber, the MO Subscriber Handset 102, and the electronic transaction device application. This PIN will be matched internally to the unique MO Subscriber Handset 102 identification number PIN and error message generated for incorrect PIN. The entry of a PIN also provides user validation for a "Card Holder Present" transaction. This sequence typically will not be repeated after the initial setup is completed successfully. On subsequent uses, only electronic transaction device PIN is required. This sequence may be performed off-line.

In step 188 the MO subscriber selects payment vendor and type, and in step 190 enters a payment PIN. A Payment PIN may be pre-assigned by Payment Vendor. A Payment vendor may create a "Digital Signature" for every account and/or PIN created at the server. On verification of Payment PIN, step 192, the server will download the card details to the MO Subscriber Handset 102. The card details may include the digital signature. The digital signature is stored locally on the MO Subscriber Handset 102 for subsequent use. This sequence may be performed on-line.

In step 194, the MO subscriber may then select a type of MO pre-paid card (Gold, Platinum, etc.) and in step 196 an amount for the pre-paid card. The MO Subscriber Handset 102 with ETD application may dial out to the Wallet Service Provider and/or MO Server and download Pre-Paid Account details from the Server.

This unique pre-paid account detail is stored on the MO Subscriber Handset 102 for subsequent use.

When the MO subscriber confirms payment in step 198, The MO Subscriber Handset 102 with ETD application may dial out to the Wallet Service Provider, debit the Payment account with the amount selected, and credit the Pre-Paid account at the WSC / MO server in step 200. A receipt acknowledging the request and confirming payment may be returned to the MO Subscriber Handset 102.

The Airtime minutes available, available Credit with the Payment Partner and Receipt for the transaction may all be stored on the device. Real time data is obtained from the respective servers during on-line sequence. All subsequent computations may be internal to the MO Subscriber Handset 102 having the ETD application.

Referring to Figure 9, an example of a credit card payment top off sequence flow chart is illustrated. The MO subscriber activates an ETD icon on the MO Subscriber Handset in step 202, and then enters a PIN in step 204. The PIN is verified as correct in step 206. The PIN is "tied-up" to the SIM Card on the MO Subscriber Handset 102. The PIN entered is matched to the PIN stored in the ETD application during the setup sequence, illustrated in Fig. 8.

In step 208, display may be activated to display current airtime available for use. In step 210, the MO subscriber may be queried as to whether to top off the pre-paid account. If yes, the MO subscriber may select the top off amount in step 212, select payment and vendor type in step 214, and enter a payment vendor PIN in step 216. PINs may be different for different payment vendors.

In step 218, if the PIN is correct, payment is confirmed in step 220. "PIN & Pay" triggers transmission of Digital Signature/Payment Account details stored on the device, along with the amount selected in step 222. This encrypted and secure

information is sent to the WSC/Payment server. On verification, the amount is debited from the Payment Server & credited to the MO Pre-paid Server. This may be the only on-line activity during the "top-off" sequence.

Figures 10 & 11 illustrate some User Interface screens on the MO Subscriber Handset 102. Referring to Figure 10, a first screen display 224, the user interface may include a graphical log for the electronic transaction device 226, a logo for the MO 228, and a log for the Payment vendor 230. A second screen display 232 may include a graphical image of a pre-paid card 234 and icons for talk time 236, top-off 238, set up 240, and exit 242. A third screen display 244, which may be displayed when top-off is selected, includes a MO pre-paid card image 248 with icons 248 for selecting a value to purchase. Additional displayed icons include talk time 236, top-off 238, Cancel 250, and main 252. A Fourth screen display 254 may be displayed after an amount is selected. The fourth screen display includes a MO Pre-paid card image 256 having icons for calling credit 258, service credit 260, and combination 262. An additional icon is a Buy icon 264.

Once the Buy icon 264 is activated, a fifth screen display 266 (Fig. 11) may be displayed. The fifth screen display 266 may include an image of a conventional credit card 268. Icons on the fifth screen display may include available credit 270, Pay 272, Receipt 274, and Main 252.

Once the Pay icon 272 is activated, a sixth screen display 276 may be displayed. The sixth screen display 276 may display a confirmation that the transaction is complete 278, and icons for available credit 270, Pay 272, Receipt 274, and Cancel 250.

A seventh screen display 280 may include icons for receipt archives 282, available credit 270, and cancel 250. An eighth screen display 284 may include an

image of a pre-paid card 286 having a display for available air time 288. Icons for the eighth screen display 284 include talk time 236, top-off 238, set up 240, and exit 242.

Figure 12 illustrates one example of the internal architecture of the Merchant ETD 104. The Merchant ETD 104 may comprise components similar to or the same as a mobile handset – keypad 300, internal hardware, such as system microprocessor, memory software & BIOS 302, the mobile operator's connectivity interface 304 (Analog, Digital, PCS, GSM, etc.) and the wireless interfaces for proximity transmission using infrared or possibly proximity RF 306. The Merchant ETD 104, in addition to the above components typical to mobile handsets, may also have the point of sale interfaces 308 for receipt printers and other peripherals commonly used in a retail environment, such as bar-code scanners, and a modem for conventional local-line access 310. In one example, the Merchant ETD 104 is a software application installed on an existing mobile handset. In alternative examples, the Merchant ETD 104 may be a personal digital assistant ("PDA") or dedicated hardware embodiment with the above outlined modules and enabling software, to conduct secure real-time or batch transactions.

The Merchant ETD 104 includes a software application loaded into the environment, which will allow it to exchange transaction information with another mobile handset with the electronic transaction device functionality (or alternately a UET Card – PDA's, etc., with electronic transaction device functionality), using a proximity method, or using the MO. The proximity method involves the beaming of a virtual pre-paid card from the Merchant ETD 104 to the subscriber's handset, and optionally, the electronic transaction device beaming payment information back into the Merchant ETD 104. The Merchant ETD 104 has the capability to capture this transmission through its infrared or proximity RF transceivers, and process it to

complete the transaction. This information is transmitted between the two handsets using existing industry standards and protocols, but is a secure transmission. One example of a server transaction uses the exchange of public/private keys to encrypt/decrypt the data – a PKI scheme), using secure transaction technology ensuring data integrity between the two mobile handsets or devices.

Alternatively, the Merchant ETD 104 may also be programmed to securely upload or beam a "virtual pre-paid airtime card" to another mobile handset in a proximity transmission, maintaining the integrity of the mobile operator's card distribution schemes. The Virtual Card is an electronic version of the physical plastic card. The information, be it an authorization code which is scratched off or any other encoded data, would be transmitted to the Merchant ETD 104 and stored, and consequently delivered or re-transmitted to the receiving mobile handset. One possible configuration of a non-proximity model would include a series of SMS messages between the mobile operator's network and the Merchant ETD 104.

Figure 13 describes some User Interface potential screens for the Merchant ETD 104, which are based on the process flow charts detailed in Figures 5 & 6. A first display screen 320 for the Merchant MTD includes an ETD Logo 322 an a MO logo 324. A second display screen 326 includes a Form 328 for entering Merchant ID and PIN. Also included are icons for Exit 330 and Done 332.

A third display screen 334 includes a form for entry of a MO subscriber telephone number 336, icons for selecting an amount of value purchased 338, icons to select between Cash 340, Debit Card 342, Credit Card 344, or Other 346, and Icons for Previous 348 and Done 332. A Fourth display screen 350 includes a icon to select Mobile Operator 352 and an icon to beam a virtual card 354. A Fifth screen display 356 includes a display of the airtime available 358 for the given telephone number.

The Fourth display screen 356 also includes a display confirming completion of the transaction 360. On the MO subscriber handset, a screen display 362 including an identification of the Mobile Operator and logo 364 and available airtime 366 may be displayed.

Figure 14 illustrates one example of the architecture of the Wallet Service Center (WSC). The WSC connects to the MO Subscriber handsets or electronic transaction devices through the MO switch. The WSC also has interfaces to the MO servers and databases, the Banks or Payment Partners, the Merchants (retail, "e or m-tailers") and Content Providers. The WSC may use a PKI/wPKI based security scheme to secure all the information being transmitted between the various entities outlined above. Some of the core features of the WSC are to support electronic transaction device users and allow all users to create a personalized transaction portal - allow them to archive all transaction records, and setup personal, financial and health information. The WSC, based on the rich profiles it creates, then offers various value added services, such as Personal Services, Financial Services, Health Services, Merchant & Vendor Services, Business to Business Services, and Government, Corporate and Educational Services.

Figure 15 illustrates an example of a "Virtual Card" Generation & Download. A "Virtual Card" is an electronic version of plastic cards. The Virtual Card is a digital representation of the information which would be conventionally stored on a magnetic stripe, or smart card chip, or a bar code, etc., of a plastic card, along with the logo and branding information securely stored to prevent unauthorized duplication. This information may then be wirelessly transmitted to the MO Subscriber Handset 102, PDA, etc. with electronic transaction device application. The "Virtual Card" generation module 320 is responsible for the creation of Virtual Cards. In one

example (labeled A), the "Virtual Card" Generation Module 320 may be hosted in the WSC. The WSC, which has access to the MOs Pre-paid Server and databases, would then create a virtual pre-paid card. This virtual pre-paid card may then be downloaded, or transmitted wirelessly using the MO's Switch to the Merchant ETD 104, or alternately directly into the subscriber's mobile phone. Secure batches of virtual pre-paid cards may be created and downloaded to the Merchant ETD 104, to then be distributed wirelessly by the Merchant ETD 104 using a proximity method (as outlined in Figures 4 & 6).

In another example, the Virtual Card generation module may be hosted outside the WSC, but within the MO's Network (labeled B). As may be the case with the generation of Credit Cards, Debit Cards, etc., the Banks and Financial Institutions may not be comfortable with another entity issuing their cards. In such a case, the Virtual Card generation module would be integrated with the Bank's or Financial Institution's payment server. These cards may still be wirelessly downloaded through the MO's Switch.

Figure 16 describes a "Stored Value Application." Similar to the examples illustrated in Fig. 3 to setup or replenish a pre-paid airtime account (or disable), the mobile operator may setup a stored value account for their subscribers in a MO stored value server and database 372. While a mobile telephone account is used as an example, the use of stored value cards is not limited to telephone applications. For example, stored value cards may be used for cash payments in proximity transactions, such as, but not limited to, vending machines, tolls, parking, and transportation.

The Wallet Service Center 112 may create and manage separate accounts for the MO Subscribers. For example, the Wallet Service Center 112 may create a stored value account, where the MO Subscriber would create a debit account by depositing

funds with the mobile operator. The MO Subscriber may then purchase goods from a merchant that uses a Merchant ETD through the examples described earlier e.g., by using a proximity transaction method or using the MO Switch. For example, the MO Subscriber may purchase products and services provided by the merchant including, but not limited to, pre-paid airtime, using the MO Subscriber ETD 106. As in the examples given above, and in the examples that follow, the MO Subscriber ETD 106 may be embedded in the MO Subscriber Handset 102. The merchant follows the same methods described earlier, with the additional step of deducting the amount of the transaction from the stored value account the subscriber creates with the mobile operator.

The authentication of the transaction may involve both the merchant and the MO Subscriber through, for example, a messaging system operated by the mobile operator. A record of the transaction may be provided by the WSC, and/or through the mobile operator's messaging service. In another example, the Merchant ETD transfers a record of the transaction to the MO Subscriber ETD 106. The Wallet Service Center may create and track this account for the mobile operator, as the MO Subscriber uses the funds from this account to pay for products and services purchased from merchants.

In another example, MO Subscribers having a stored value account may obtain a cash advance from the Merchant ETD. In this example, the MO Subscriber liquidates a certain amount of the debit (or credit) account previously setup with the mobile operator. The Merchant ETD effectively becomes an ATM outlet.

In addition to the stored cash value accounts, the mobile operator may decide to add a credit functionality to this process, and become a credit account vendor as well.

The billing in any of these examples may be in the form of a consolidated or separate statements from the mobile operator. The consolidated statement details the airtime used followed by a section that details how the stored value account was depleted. Separate statements, on the other hand, provide separate statements for telephone usage and stored value account usage. The Wallet Service Center may use the mobile operator's messaging system to update the MO Subscriber ETD 106 with balance information. As in the above examples, the ETD may be embedded in a MO Subscriber Handset 102.

Figure 17 illustrates an example of the stored value transaction system using the mobile operator's network. MO Subscriber Handset 102 is in electronic communication with MO switch 110. A merchant POS terminal is also in electronic communication with the MO switch 110. In the illustrated example, the merchant POS is a Merchant ETD 104. Other POS equipment may be suitable. The MO switch 110 is coupled to Wallet Service Center 112. WSC is coupled to MO Stored Value Server 372, MO Prepaid Server 114, and Payment Server 116. This system does not necessarily require any modifications on the subscriber's mobile phone, but merely requires the subscriber to establish a stored value account with the mobile operator. The subscriber may setup a stored value account using, for example, the following methods:

Subscriber may deposit money at a mobile operator certified distribution outlet using cash, credit, debit, check, etc. to pay the merchant. The merchant then dials into the mobile operator's system to update the subscriber's account. The merchant may use the Merchant ETD to update the subscriber's stored value account.

The subscriber may directly access his/her account securely using the ETD to top-up his/her stored value account. The subscriber may replenish the account using a credit card, debit card, or any other acceptable payment product, from the ETD.

The subscriber may access his/her stored value account from the Internet, by paying using a credit card or a debit card.

The subscriber may pay the mobile operator directly, by including an extra payment over and above the billed amount for wireless services every month. This extra amount may then be credited to the stored value account housed by the mobile operator.

Once the MO Subscriber creates the stored value account with the mobile operator, the MO Subscriber may conduct a transaction by merely specifying the account number to the merchant with a Merchant ETD 104. The account number may be a telephone number corresponding to the MO Subscriber. Referring to Figure 18, in step 402, the MO Subscriber selects merchandise or services at a Merchant's POS location. In step 404, the merchant turns on the Merchant ETD, enters a password, enters the MO Subscriber's account details, and the amount of merchandise / services desired by the MO Subscriber. In step 406, the Merchant sends the information to the WSC, through the mobile operator's switch by the Merchant ETD. In step 408, the WSC authenticates the merchant, the MO Subscriber, and ensures that the stored value account has enough funds (alternately available credit balance, if the mobile operator offers a credit facility to the subscriber) to cover the transaction. The WSC also updates the internal databases on the merchant, subscriber and mobile operator. In step 410, once the transaction is approved, the WSC requests the mobile operator to send a unique transaction ID, for security purposes, in the form of a short message (if service available) to both the merchant and the MO Subscriber, completing the

transaction. In step 412, the Merchant acknowledges the MO Subscriber's payment. In step 414, the MO Subscriber received a message, for example, a SMS message, from the WSC specifying the new balance in the stored value account.

Figure 19 illustrates a proximity transaction based stored value system. MO Subscriber ETD 106 (which may be embedded in MO Subscriber handset 102) is in electronic communication with a merchant POS terminal. In the illustrated example, the merchant POS is a Merchant ETD 104. Other POS equipment may be suitable. The Merchant ETD is in electronic communication with MO switch 110, which is in turn coupled to Wallet Service Center 112. WSC is coupled to MO Stored Value Server 372, MO Prepaid Server 114, and Payment Server 116.

Referring to Figure 20, in use, the WSC distributes electronic, or virtual, stored value cards in step 420. The virtual stored value cards may be distributed directly to the MO Subscriber ETD. Alternatively, the virtual stored value cards may be distributed to the Merchant ETDs. Mobile operator certified distributors may be authorized to distribute these cards on a proximity basis to subscribers. These cards may be purchased at retail locations. In other examples, stored value accounts may be replenished using the methods described above to top off prepaid accounts. The virtual stored value cards may be issued wirelessly and securely, and may be stored in the MO Subscriber ETD, containing user information, issuer information, amount details, and other authentication information.

In step 422, to conduct a transaction using the stored value card, the MO Subscriber selects the card in the ETD, and transfers the desired amount into the merchant POS. Any suitable electronic communication may be used for the transfer, including, but not limited to, infrared or proximity RF. In step 424, the Merchant ETD authenticates the MO Subscriber's virtual stored value card and transfers a

receipt of the transaction to the MO Subscriber ETD. In step 426, the merchant uploads relevant transaction information to the stored value server hosted by the WSC and the mobile operator. The upload may be performed at a later time in a batch of transactions. In step 428, the WSC updates the MO Subscriber's stored value account information. In step 430, the WSC updates the internal merchant, mobile operator, and subscriber databases.

The stored value system described herein provides a secure and cost effective transaction network. In part because the stored value system is hosted by the mobile operator and the WSC, wireless transactions are enabled. Also, by using the mobile operator's network, the administration cost of the transaction may be significantly reduced as the number of intermediaries is reduced. The WSC, along with the ETD and the Merchant ETD ensure end to end security, and global deployment. Since authentication may be enforced by the ETD and Merchant ETD at the POS, this system may drastically reduce fraud. The WSC, through its profiling capabilities, can reduce the customer acquisition costs.

The Merchant ETD may be deployed in markets where the existing banking networks do not have a presence, consequently increasing transaction volume for existing banking entities involved in the deployment of this solution. The stored value systems may be effectively extended to minors and credit challenged individuals, again increasing the addressable markets and consequently transaction volume. This system may also be extended for people to people payments, where two individuals with ETD's may transact directly on a proximity basis. The stored value system will also reduce cash transactions and associated costs. Even in markets where the transactions are predominantly cash based, the Merchant ETD, along with the tracking capabilities may be used to reduce fraud and theft.

Figure 21 illustrates an environment in which a single Merchant ETD 104 has the capability to interface with multiple mobile operator networks for the purposes of offering electronic pre-paid airtime or stored value applications, as outlined before, to their respective subscribers. An example would be a single merchant location, enabled with a single Merchant ETD unit, having the capability to electronically issue pre-paid airtime to Sprint PCS, Cellular One, AT&T, PrimeCO, Bell Atlantic, Bell South, etc. subscribers. This same Merchant ETD would also have the capability to allow all the different subscribers to use their respective stored value accounts hosted by the respective mobile operators.

Figure 22 illustrates examples of user interface screens for the Merchant ETD 104 in a Multiple MO environment. In a first screen 440, icons for a plurality of MO's 442 are displayed. In a second screen 444, a form for entering Merchant Identification and PIN 446 is displayed, along with icons for Exit 448 and Done 450. IN a third screen 452, a form for entry of the MO Subscriber telephone number 454 is displayed. Also displayed are icons for selecting an amount of value paid 456, and icons for form of payment, e.g., Cash 458, Credit Card 460, Debit Card 462, or Other 464. Additional displayed icons include Previous 466, and Done 450. In a fourth screen 468, icons for selecting between MO's 470 are displayed. Also, an icon for transferring the virtual card 472 is displayed.

Figure 23 describes an existing transaction system and a wireless transaction system. One of the purposes of this patent is to introduce a new transaction system, which includes the Merchant ETD at the POS (and possibly the ETD, in certain embodiments), along with the Wallet Service Center. The existing transaction system typically consists of a POS 380, or retail environment. This is connected, through a secure banking network 382 to the acquirers 384 and eventually back to the issuer 386

of the payment product – Credit Cards, Bank Cards, Debit Cards, etc. The acquirers 384 and issuers 386 may possibly be controlled by the same organization, or may be different entities bound by an arrangement to clear transactions – American Express and DISCOVER are examples of the first kind, MasterCard and VISA are examples of the later. The new wireless transaction system consists of a Merchant ETD at a wireless POS 388, wirelessly connected to the Mobile Operator's switch 110, which in turn is connected to the Wallet Service Center 112. The Wallet Service Center may be connected either to the acquirer or directly to the issuer, or possibly both, based on the acquirer – issuer relationship. The nature of the connection between the Mobile Operator's switch, the Wallet Service Center, and the acquirer – issuer's systems may be a wired or wireless connection. The ETD, Merchant ETD and Wallet Service Center ensure the security of the transaction data as it wirelessly flows from the POS location, through the Mobile Operator's switch, eventually to the acquirer – issuer's systems.

Based on the nature of the electronic transaction device application transaction, whereby the payment information (credit card details, account number, etc.) is stored and transmitted from the mobile handset, only after being initiated by the user (user enters unique password, which along with a unique handset device number – SIM, WIM, etc. – is translated into a unique key, or treated as a "digital signature" to validate the transaction) – the transaction is of a "Card Holder Present" nature. The electronic transaction device application allows the subscriber to use a credit card to setup and top-up their pre-paid account, and at the same time allows the mobile operator to pick up the savings of the reduced credit card issuer fee for a "CHP" transaction.

Using the electronic transaction device application User Interface, the subscriber now has a simple menu driven, graphical, user friendly procedure of selecting the amount of airtime required, and the payment vendor and account (credit, debit, etc.) to be used. The electronic transaction device application on the mobile handset will also allow the subscriber to store the receipt of the transaction, show the updated airtime and payment account balances. Thus the mobile operator may now use the electronic transaction device application on mobile handsets, along with its automated system, to allow their pre-paid subscribers to setup & top-up their accounts using their handsets. This removes the requirement of a customer service representative to have a dedicated session with the subscriber, and also offers a lot less cumbersome alternative to the automated setup and top-up methods.

The Merchant ETD 104 may be used for distributing pre-paid airtime, either using the MO's network and existing mobile handsets, and later on by issuing "virtual pre-paid cards." The Merchant ETD 104 may be used in a retail environment or at the certified distribution centers – bank locations, ATMs, or over the counter locations. The Merchant ETD 104 supports cash, credit card, debit card, etc. transactions. The Merchant ETD 104 allows the mobile operator to immediately reduce all costs associated with the generation, packaging and distribution of physical plastic cards. The Merchant ETD 104 also allows the mobile operator to remotely issue and track the distribution of their pre-paid products, removing all costs associated with the physical tracking of inventory. This model also gives the mobile operator the flexibility to enhance the services and products, and at the same time rapidly deliver these new offerings to their subscribers.

The same set of advantages applies to the merchants in the retail and virtual (e & m-tailers) environments. The mobile operator may use the Merchant ETD 104 to

distribute pre-paid "Virtual Cards", thereby immediately reducing all costs associated with the generation, packaging and distribution of plastic. Since the Merchant ETD 104 eliminates the requirement of shelf space, and also removes the element of "physical inventory management" on the retailers part, the mobile operator is essentially in a position to negotiate reduction in retailer margins.

The Merchant ETD 104 may also be used to enhance or upgrade the current offering of products and services, and rapidly and remotely deliver these to their subscribers, with minimal costs associated. Add to these savings, the savings associated with the card holder present transaction, when the electronic transaction device application is used by the subscriber, and subsequently reduction in cash handling costs, etc.

In conjunction with the electronic transaction device application and Merchant ETD 104 products, the Wallet Service Center (hereby incorporated by reference) also allows the mobile operator to create a trail of otherwise untraceable "cash" transactions/subscribers. This is beneficial in terms of allowing the mobile operator to better understand their subscribers and cater additional products and services to them. This also, in light of law enforcement requirements by government agencies, allows the mobile operator and law enforcement agencies to track unlawful use of pre-paid phones.

In summary, present invention is that it allows MO's to extract more value, and hence immediate profitability, from their existing distribution models – be it in terms of eliminating cost of producing and distributing plastic, or the high commission paid to the retailers, or the CHP nature of all credit card transactions. The present invention allows the mobile operator to create alternate distribution

channels, giving them the ability to modify each existing mobile handset into a potential point of sale terminal.

The electronic transaction device application gives the mobile operator the presence on the subscriber's handset, the Merchant ETD 104 gives them the ability to distribute products and services in a retail environment, essentially taking the mobile operator beyond the m-commerce space. The WSC gives the mobile operator the ability to continuously keep adding on value added services for their subscribers, merchants and vendors. Thus, the mobile operator now has the ability to create a trace of their subscribers, including the subscribers that typically pay cash and leave no personal information behind. The WSC creates a profile for each subscriber, whether they use cash or credit cards, or debit cards, etc. to pay for the pre-paid airtime. This is also helpful for the law enforcement agencies to curb the misuse of pre-paid phones for unlawful activities. In addition, the WSC allows the mobile operator to efficiently track the airtime top-up for all their subscribers, independent of who the subscriber is or how they purchased their pre-paid airtime. The WSC creates a better and more efficient management system between the mobile operators and various distributors they use in the retail and non-retail environment.

The WSC, along with the electronic transaction device application and Merchant ETD 104, creates the optimum platform for the mobile operator to offer various value added services and products to their subscribers, merchants and services. The stored value application is an example of how the mobile operator may use the same infrastructure installed to electronically distribute pre-paid airtime, to allow their subscribers to buy products and services from the merchants equipped with a Merchant ETD.

The new wireless transaction system introduced, which includes the ETD, Merchant ETD and Wallet Service Center, would now make the entire transaction more secure and profitable. In one embodiment, the ETD securely and wirelessly transmits the payment information from the user to the Merchant ETD, or directly to the WSC. In another embodiment the Merchant ETD directly relays the transaction data to the WSC. Both these configurations reduce the element of fraud at the POS, where now the user of the ETD, or the merchant using the Merchant ETD are authenticated. The transaction data is also securely transmitted from the user to the POS to the acquirer – issuer's system, with less intermediaries, reducing the potential of fraud. The new system also reduces the cost of a transaction by reducing the intermediaries, thereby allowing the acquirer – issuers to channel the cost savings back to the user.

What is claimed is:

1. A method of exchanging payment information in an electronic transaction, comprising:

a) a first electronic transaction device transferring payment information to a second electronic transaction device;

b) the second electronic transaction device transferring value information to the first electronic transaction device;

c) the second electronic transaction device transferring value information and payment information to a service consolidation center.

2. The method of claim 1, wherein the value information comprises a virtual card.

3. The method of claim 2, wherein the virtual card comprises an authorization code.

4. The method of claim 2, wherein the virtual card comprises an image of a card.

5. The method of claim 1, wherein the value information comprises a quantity of minutes corresponding to a pre-paid telephone account.

6. The method of claim 1, wherein the payment information comprises cash payment information.

7. The method of claim 6, wherein the cash payment information includes an identification of a person providing a cash payment.

8. The method of claim 1, wherein the payment information comprises credit payment information.

9. A method of tracking retail sales of pre-paid telephone cards to cash subscribers comprising:

a) entering value purchased information and subscriber information in a retailer electronic transaction device;

b) the retailer electronic transaction device transferring the value purchased information and subscriber information to a mobile operator;

c) the mobile operator adding value corresponding to the value purchased information to an account corresponding to the subscriber information.

10. The method of claim 9, wherein the step of entering value purchased information and subscriber information in a retailer electronic transaction device further comprises electronically transferring the value purchased information and subscriber information from a MO subscriber handset to the retailer electronic transaction device.

11. The method of claim 9, wherein the step of entering value purchased information and subscriber information in a retailer electronic transaction device further comprises manually entering the value purchased information and subscriber information into the retailer electronic transaction device.

12. A method of distributing virtual pre-paid cards comprising:

a) creating a virtual pre-paid card;

b) downloading the virtual pre-paid card to a retailer electronic transaction device,

c) transferring the virtual pre-paid card from the retailer electronic transaction device to a MO Subscriber Handset 102.

13. The method of claim 12, further comprising the step of transferring payment information from the MO subscriber handset to the retailer electronic transaction device.

14. The method of claim 12, wherein the step of creating a virtual card is performed by an electronic transaction device service center.

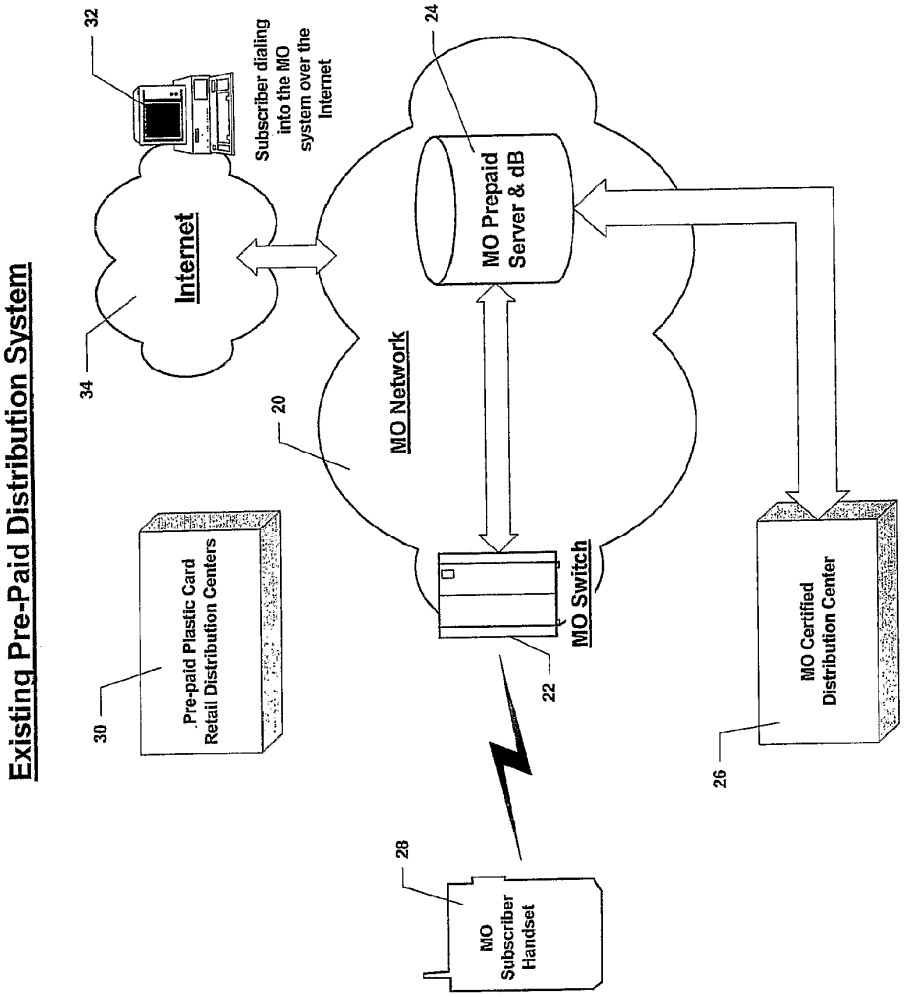
15. The method of claim 14, further comprising the steps of:

a) transferring payment information and subscriber information from the MO subscriber handset to the retailer electronic transaction device; and

b) transferring the payment information and subscriber information from the retailer electronic transaction device to the electronic transaction device service center.

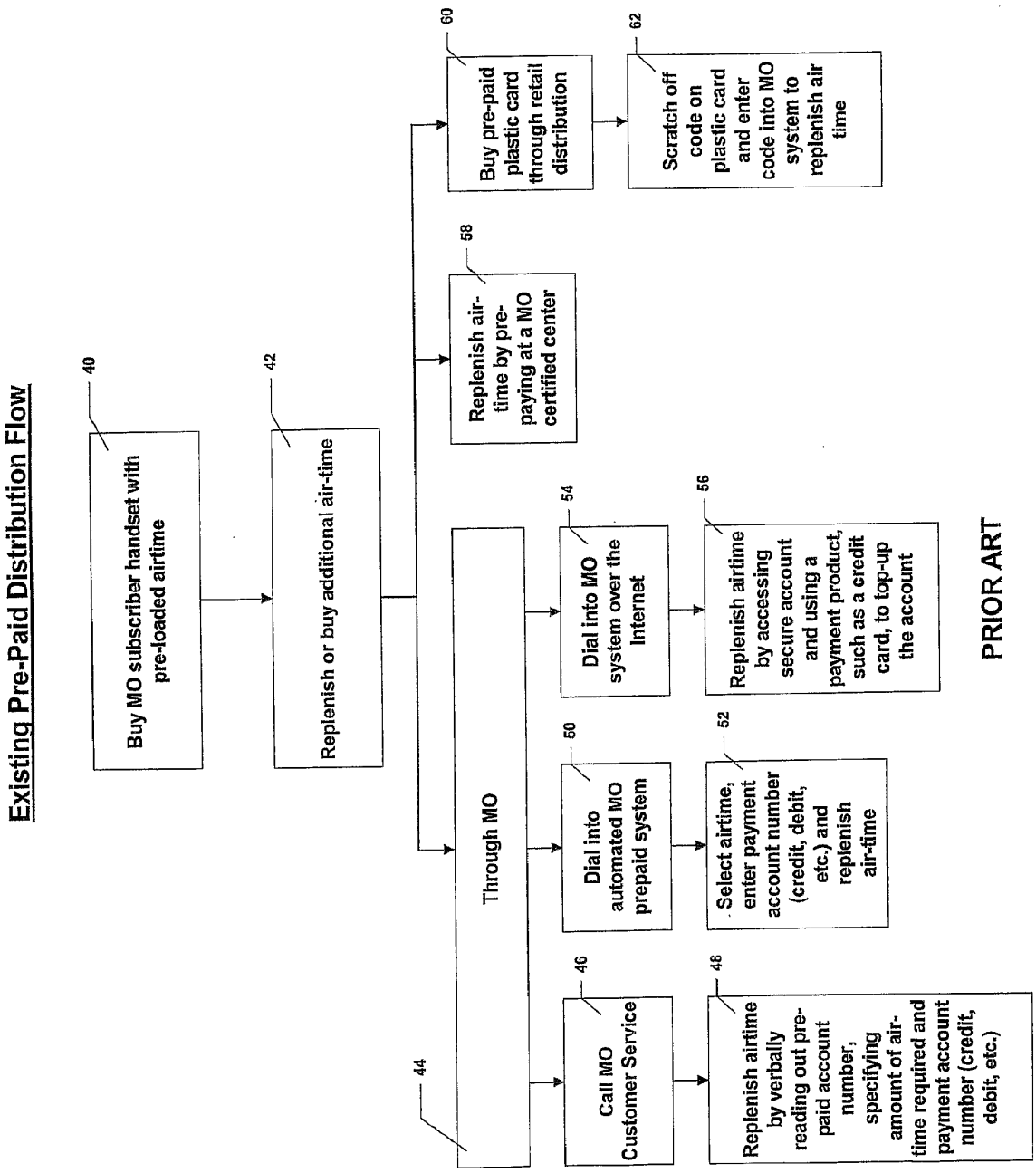
16. The method of claim 14, wherein the step of downloading the virtual card to a retailer electronic transaction device occurs via a MO switch.

17. The method of claim 12, wherein the step of creating a virtual card comprises creating a plurality of virtual cards and the step of downloading the virtual card to a retailer electronic transaction device comprises downloading batches of virtual transaction cards to the retailer electronic transaction device.



PRIOR ART

Figure 1



PRIOR ART

Figure 2

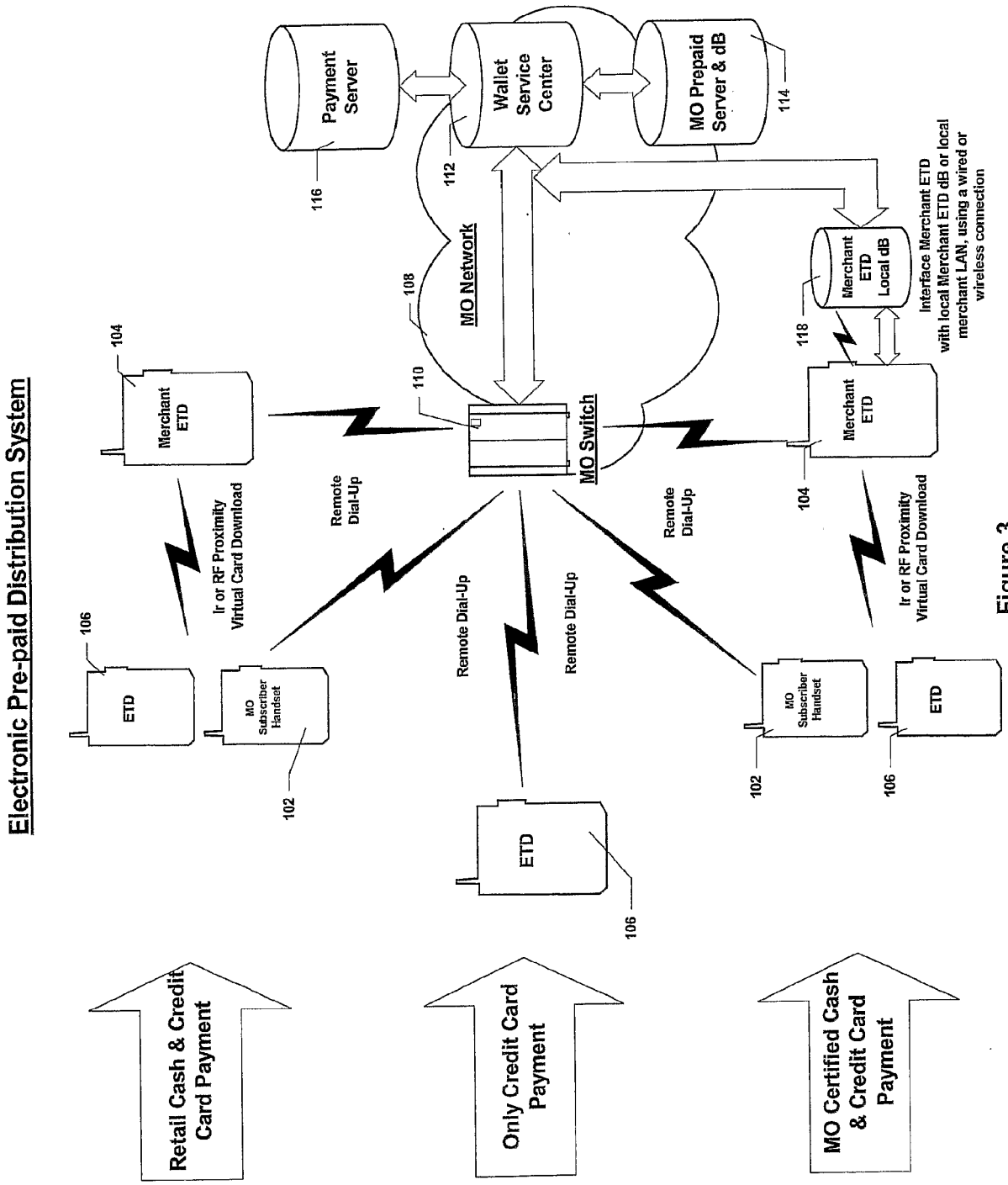

Electronic Pre-paid Distribution System
Payment Server
Wallet Service Center
MO Prepaid Server & dB
116
112
114
MO Network
108
Merchant ETD Local dB
Interface Merchant ETD with local Merchant ETD dB or local merchant LAN, using a wired or wireless connection
118
104
Merchant ETD
110
MO Switch
Merchant ETD
104
Ir or RF Proximity Virtual Card Download
Remote Dial-Up
Remote Dial-Up
Remote Dial-Up
Remote Dial-Up
Ir or RF Proximity Virtual Card Download
106
ETD
MO Subscriber Handset
102
Retail Cash & Credit Card Payment
Only Credit Card Payment
MO Certified Cash & Credit Card Payment

Figure 3

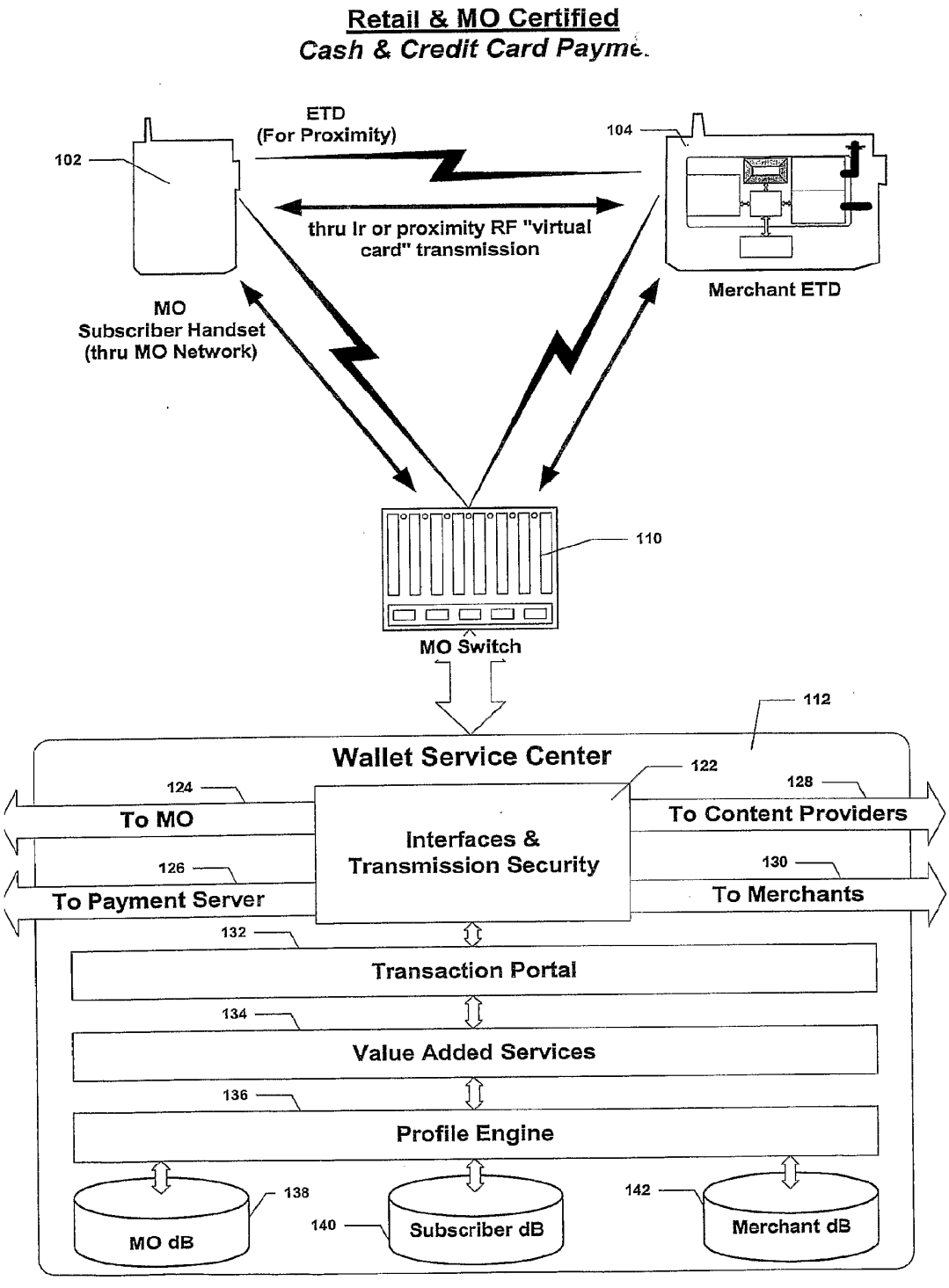

Retail & MO Certified
Cash & Credit Card Payme
ETD
(For Proximity)
102
104
thru Ir or proximity RF "virtual card" transmission
MO
Subscriber Handset
(thru MO Network)
Merchant ETD
110
MO Switch
112
Wallet Service Center
122
124
To MO
128
To Content Providers
Interfaces &
Transmission Security
126
To Payment Server
130
To Merchants
132
Transaction Portal
134
Value Added Services
136
Profile Engine
138
MO dB
140
Subscriber dB
142
Merchant dB

Figure 4

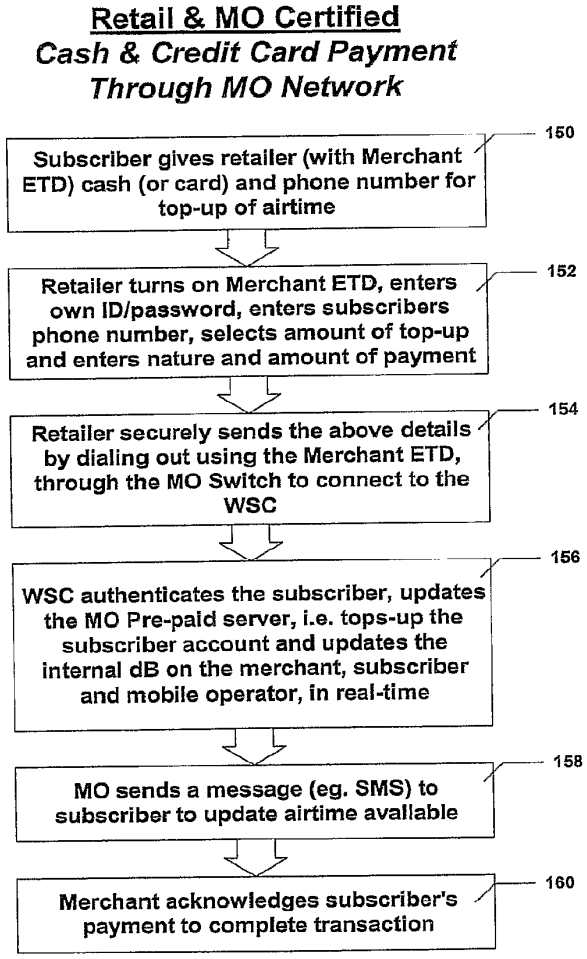

Retail & MO Certified
Cash & Credit Card Payment
Through MO Network
Subscriber gives retailer (with Merchant ETD) cash (or card) and phone number for top-up of airtime
150
Retailer turns on Merchant ETD, enters own ID/password, enters subscribers phone number, selects amount of top-up and enters nature and amount of payment
152
Retailer securely sends the above details by dialing out using the Merchant ETD, through the MO Switch to connect to the WSC
154
WSC authenticates the subscriber, updates the MO Pre-paid server, i.e. tops-up the subscriber account and updates the internal dB on the merchant, subscriber and mobile operator, in real-time
156
MO sends a message (eg. SMS) to subscriber to update airtime available
158
Merchant acknowledges subscriber's payment to complete transaction
160

Figure 5

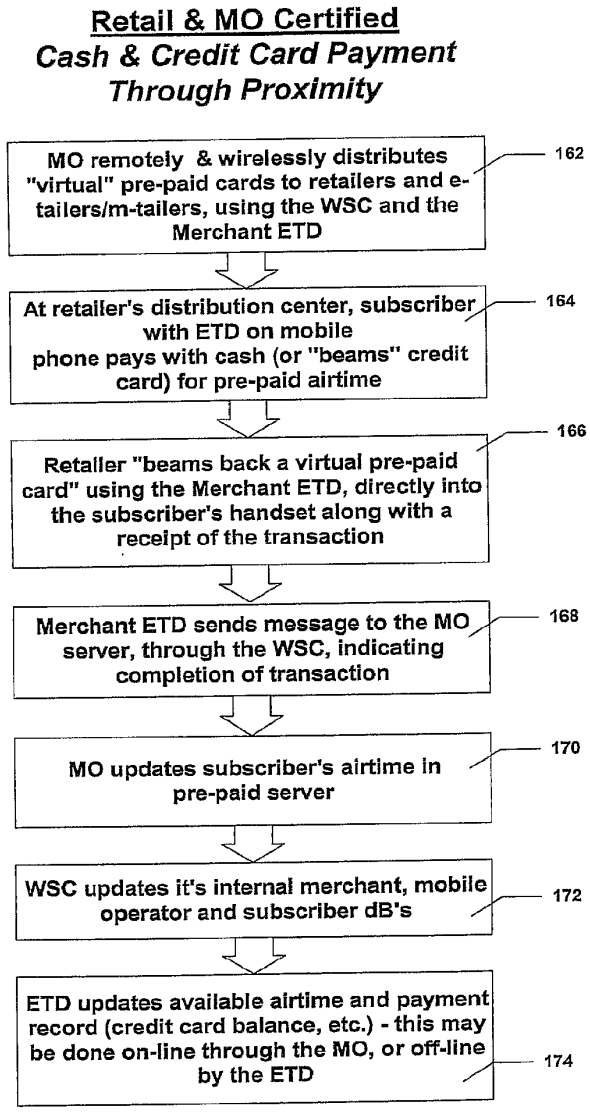

Retail & MO Certified
Cash & Credit Card Payment
Through Proximity
MO remotely & wirelessly distributes "virtual" pre-paid cards to retailers and e-tailers/m-tailers, using the WSC and the Merchant ETD
162
At retailer's distribution center, subscriber with ETD on mobile phone pays with cash (or "beams" credit card) for pre-paid airtime
164
Retailer "beams back a virtual pre-paid card" using the Merchant ETD, directly into the subscriber's handset along with a receipt of the transaction
166
Merchant ETD sends message to the MO server, through the WSC, indicating completion of transaction
168
MO updates subscriber's airtime in pre-paid server
170
WSC updates it's internal merchant, mobile operator and subscriber dB's
172
ETD updates available airtime and payment record (credit card balance, etc.) - this may be done on-line through the MO, or off-line by the ETD
174

Figure 6

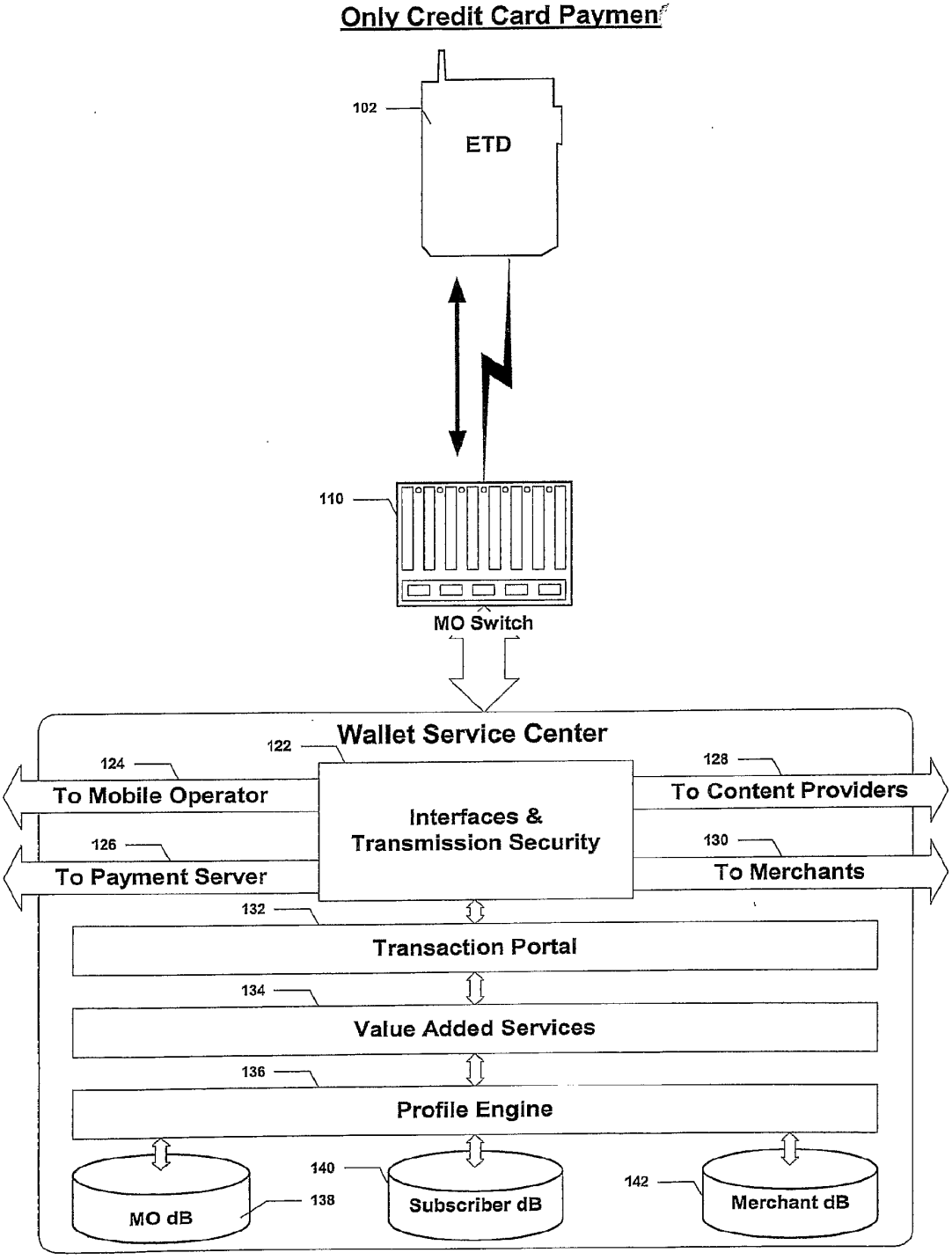

Only Credit Card Paymen
102
ETD
110
MO Switch
Wallet Service Center
122
124
To Mobile Operator
126
To Payment Server
Interfaces &
Transmission Security
128
To Content Providers
130
To Merchants
132
Transaction Portal
134
Value Added Services
136
Profile Engine
140
Subscriber dB
142
Merchant dB
138
MO dB

Figure 7

Only Credit Card Payment - Setup Sequence Flow Chart

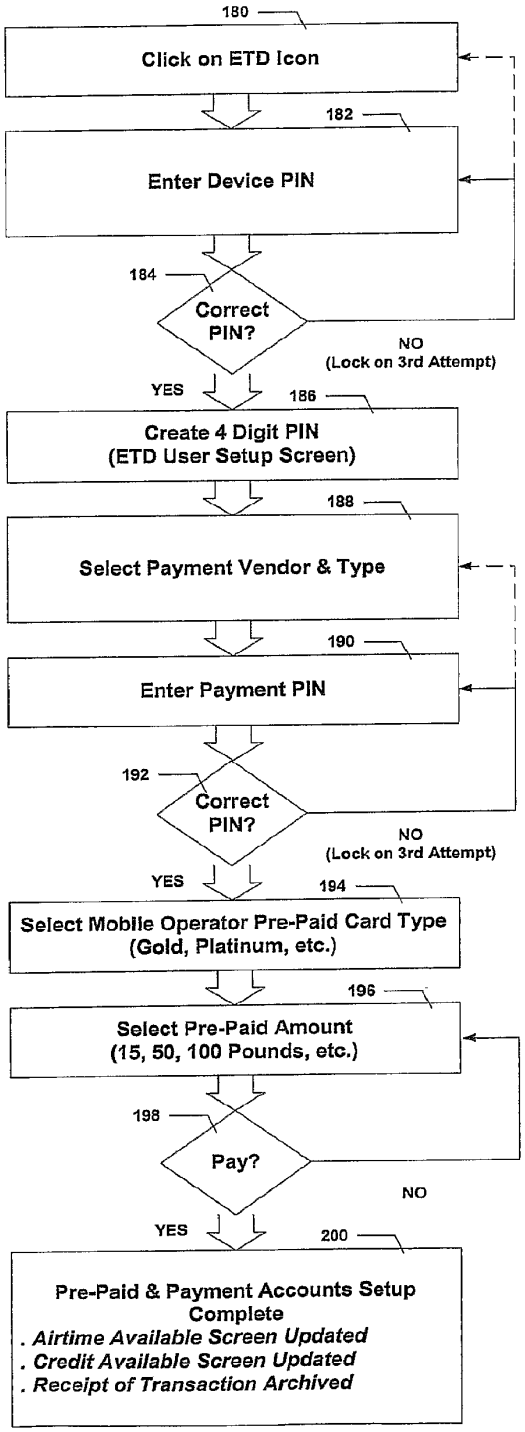


Figure 8

Only Credit Card Payment - "Top-Off" Sequence Flow Chart

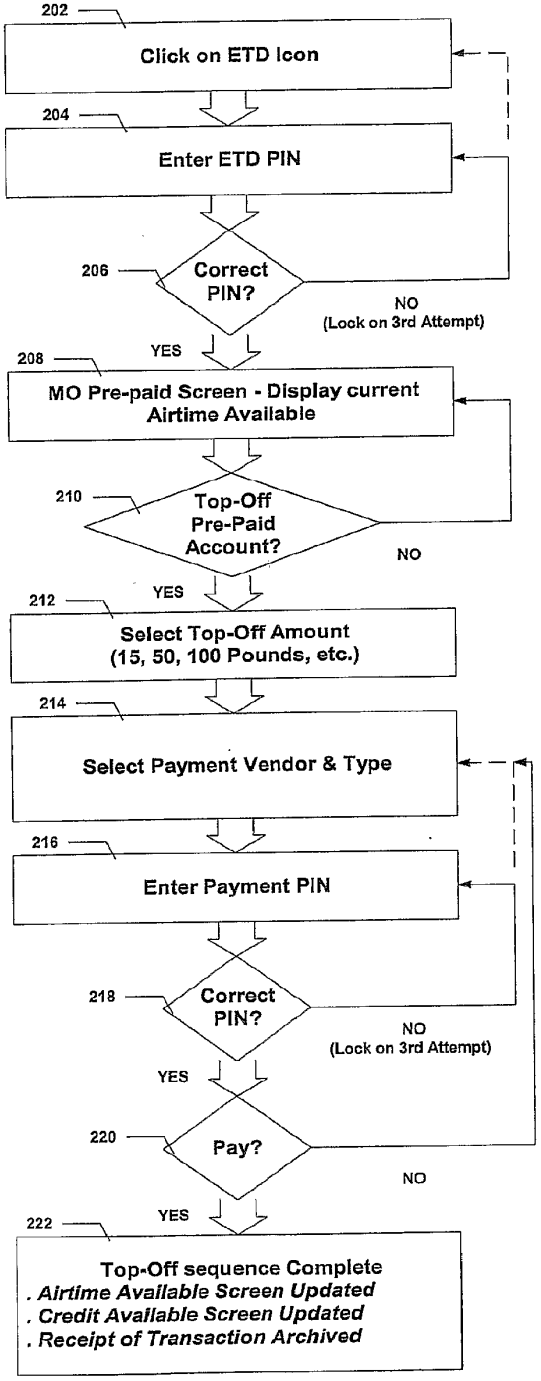


Figure 9

Only Credit Card Payment
Sample UIs

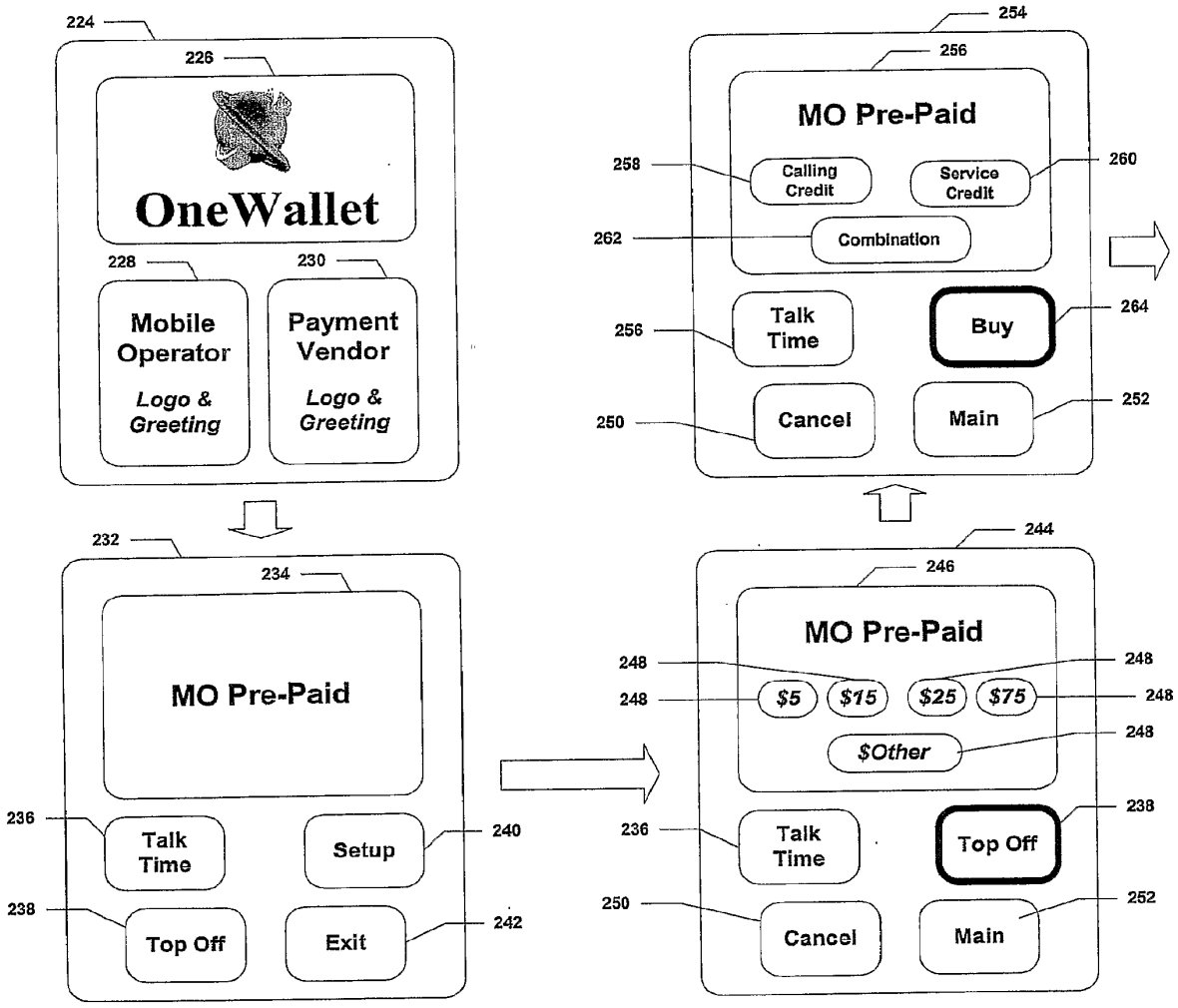


Figure 10

Only Credit Card Payment
Sample UIs

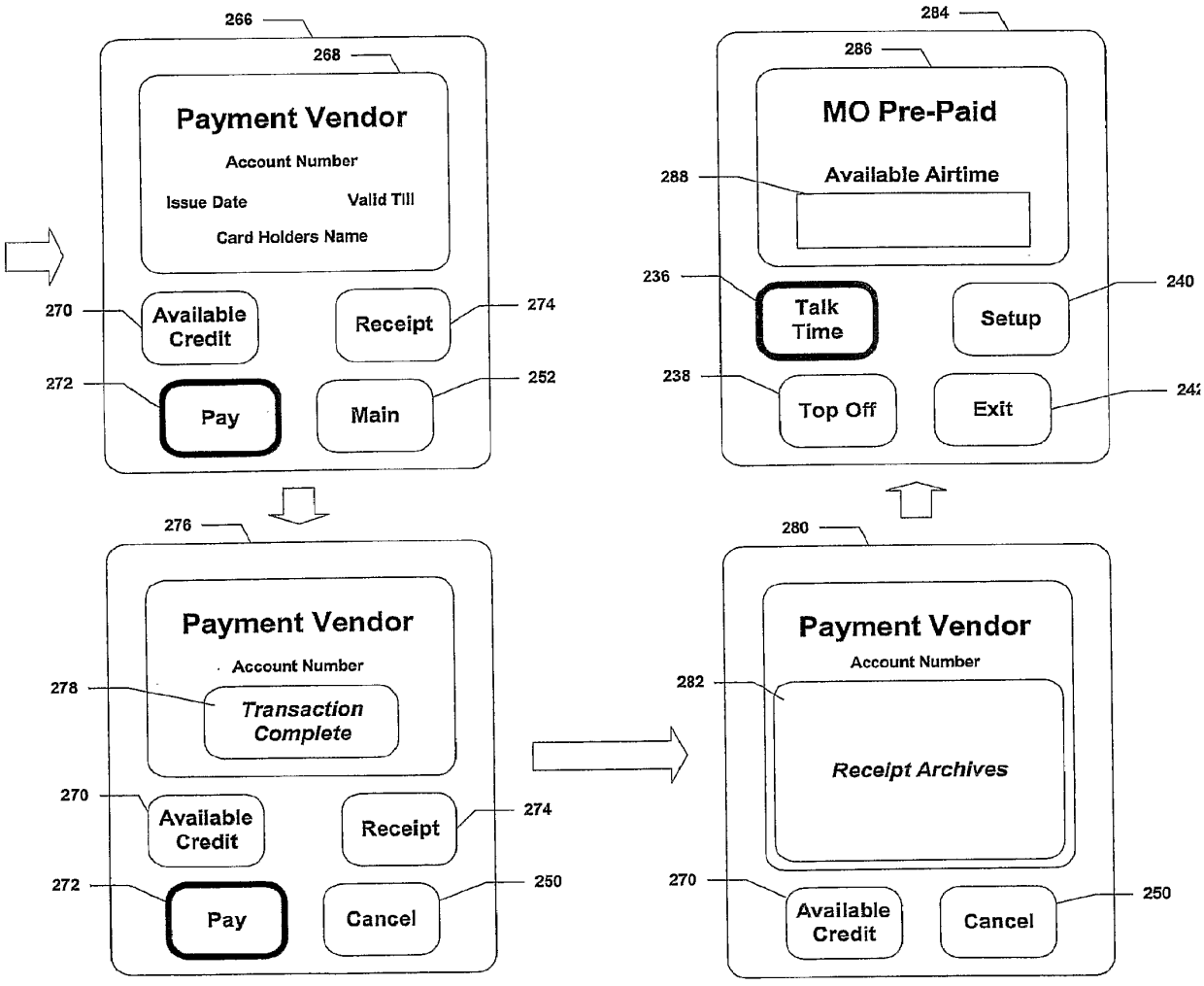


Figure 11

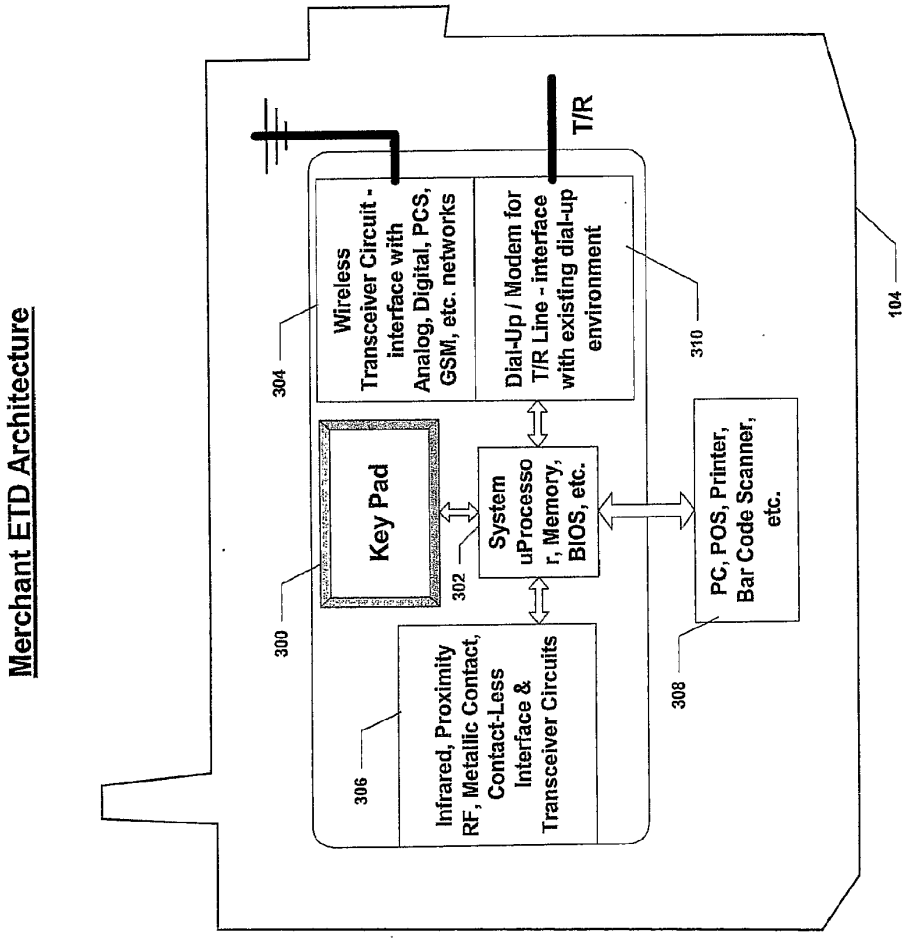

Merchant ETD Architecture
Wireless Transceiver Circuit - interface with Analog, Digital, PCS, GSM, etc. networks
Dial-Up / Modem for T/R Line - interface with existing dial-up environment
T/R
Key Pad
System uProcesso r, Memory, BIOS, etc.
PC, POS, Printer, Bar Code Scanner, etc.
Infrared, Proximity RF, Metallic Contact, Contact-Less Interface & Transceiver Circuits
304
310
300
302
308
306
104

Figure 12

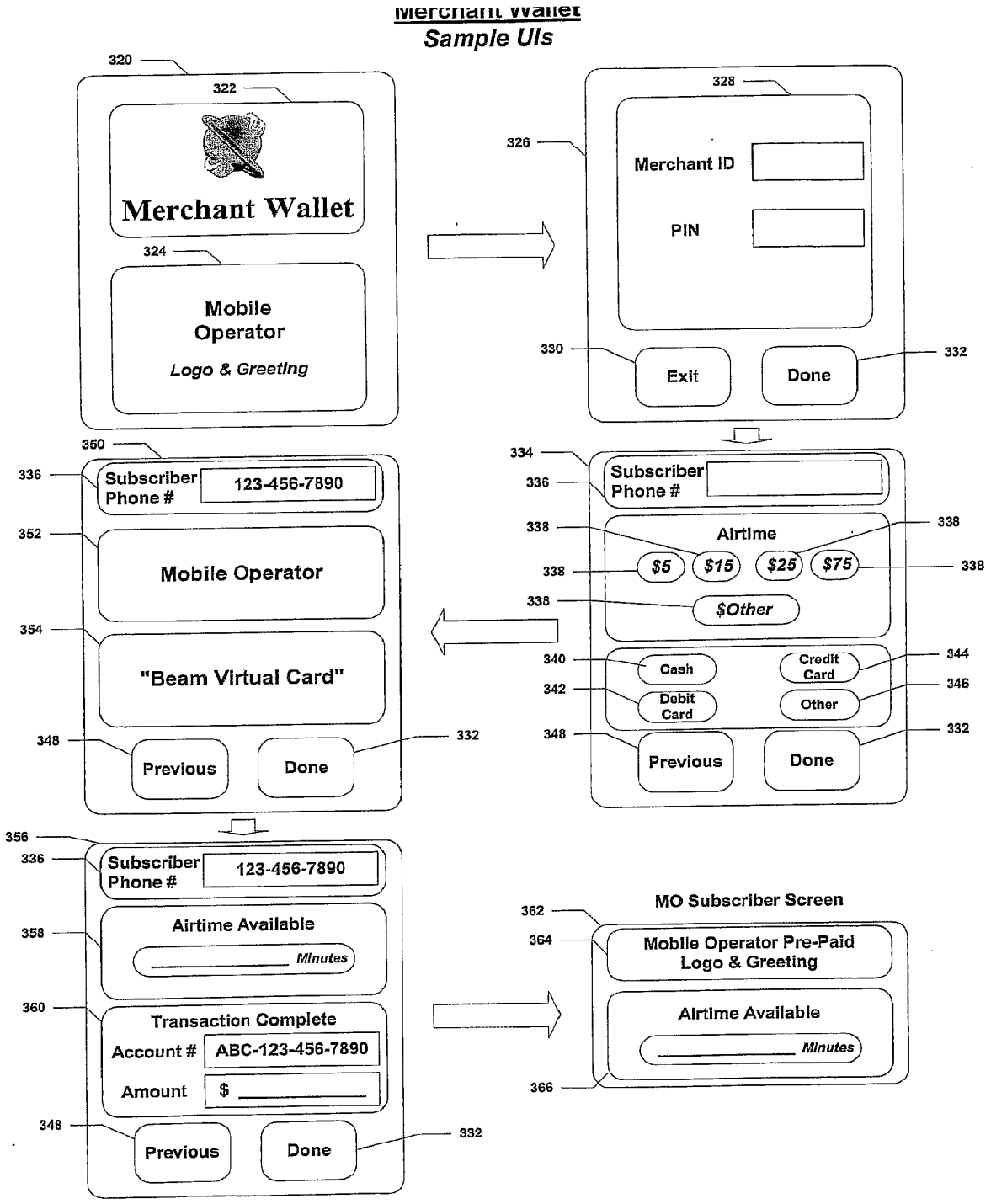

Merchant Wallet
Sample UIs
320
322
Merchant Wallet
324
Mobile Operator
Logo & Greeting
326
328
Merchant ID
PIN
330
Exit
Done
332
334
336
Subscriber Phone #
338
Airtime
$5
$15
$25
$75
$Other
340
Cash
Credit Card
342
Debit Card
Other
344
346
348
Previous
350
123-456-7890
352
Mobile Operator
354
"Beam Virtual Card"
356
358
Airtime Available
Minutes
360
Transaction Complete
Account #
ABC-123-456-7890
Amount
$
MO Subscriber Screen
362
364
Mobile Operator Pre-Paid Logo & Greeting
366

Figure 13

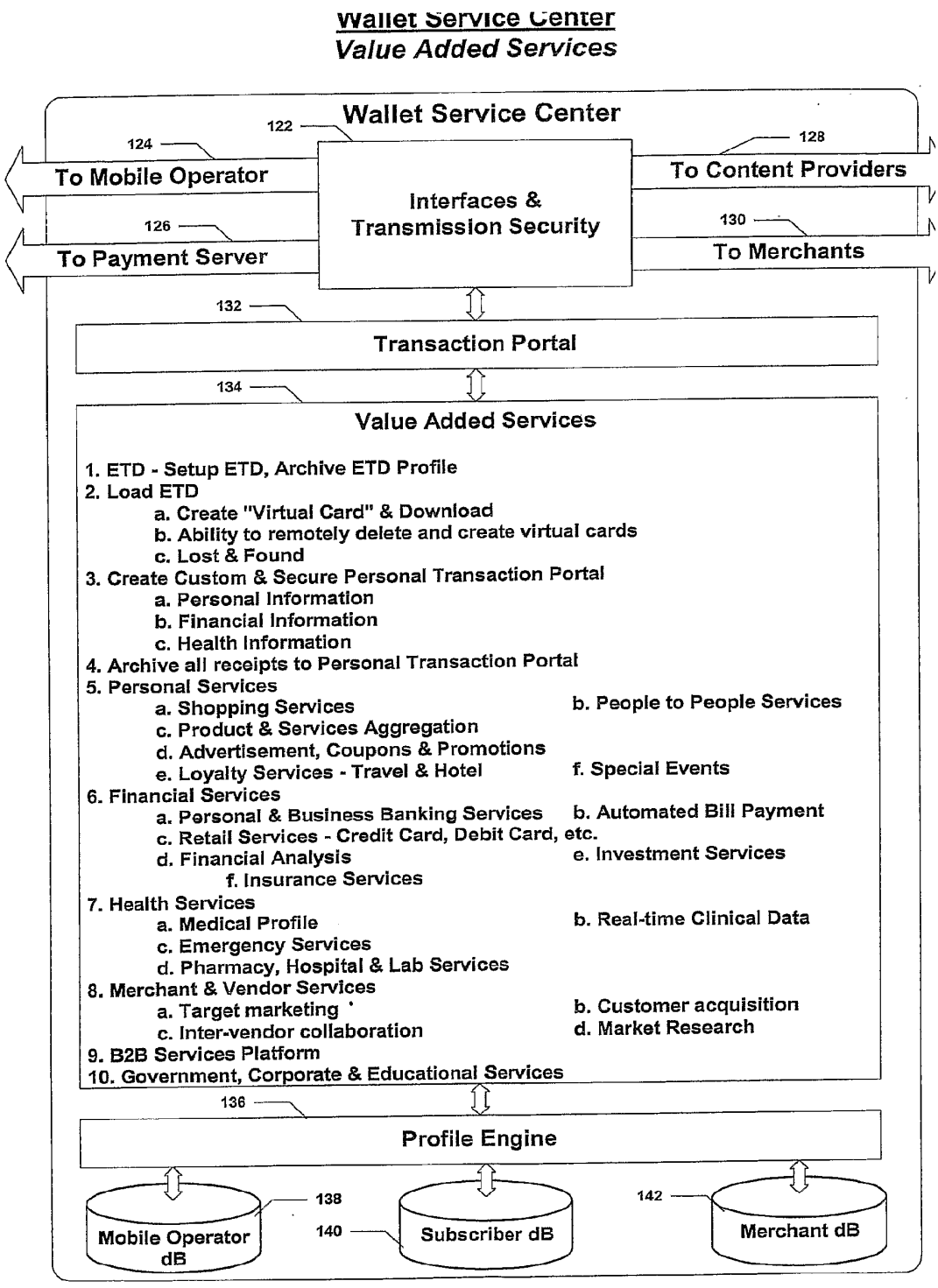
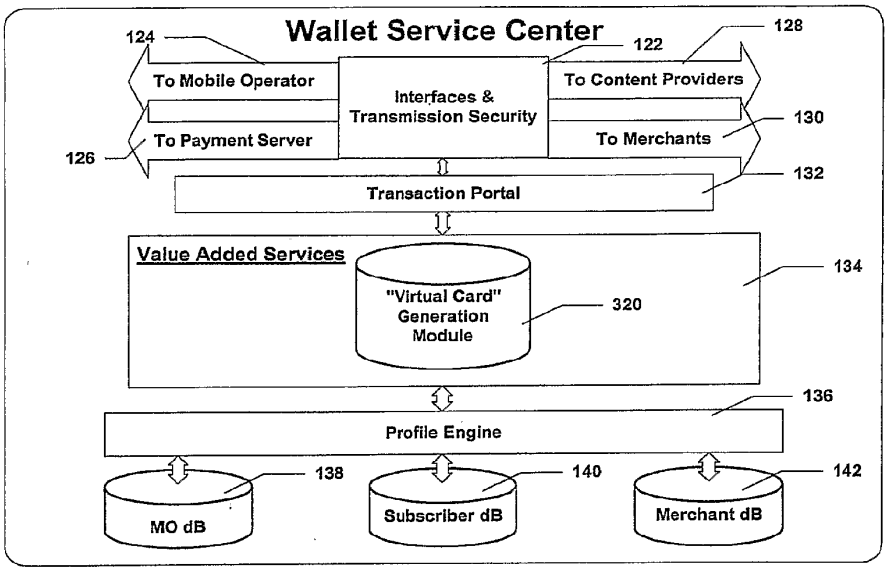
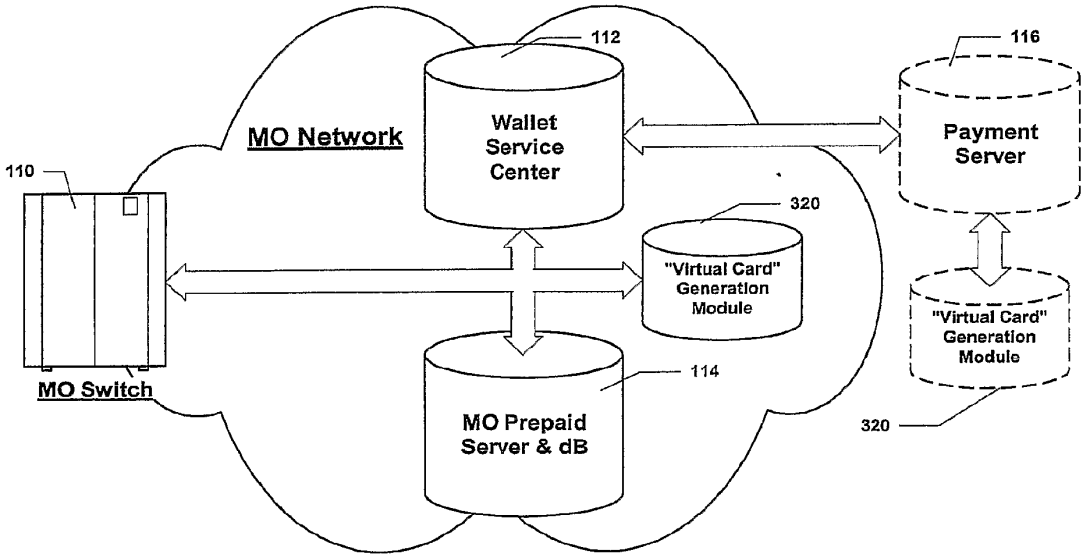

Wallet Service Center
Value Added Services
Wallet Service Center
122
124
To Mobile Operator
126
To Payment Server
Interfaces &
Transmission Security
128
To Content Providers
130
To Merchants
132
Transaction Portal
134
Value Added Services
1. ETD - Setup ETD, Archive ETD Profile
2. Load ETD
a. Create "Virtual Card" & Download
b. Ability to remotely delete and create virtual cards
c. Lost & Found
3. Create Custom & Secure Personal Transaction Portal
a. Personal Information
b. Financial Information
c. Health Information
4. Archive all receipts to Personal Transaction Portal
5. Personal Services
a. Shopping Services
b. People to People Services
c. Product & Services Aggregation
d. Advertisement, Coupons & Promotions
e. Loyalty Services - Travel & Hotel
f. Special Events
6. Financial Services
a. Personal & Business Banking Services
b. Automated Bill Payment
c. Retail Services - Credit Card, Debit Card, etc.
d. Financial Analysis
e. Investment Services
f. Insurance Services
7. Health Services
a. Medical Profile
b. Real-time Clinical Data
c. Emergency Services
d. Pharmacy, Hospital & Lab Services
8. Merchant & Vendor Services
a. Target marketing
b. Customer acquisition
c. Inter-vendor collaboration
d. Market Research
9. B2B Services Platform
10. Government, Corporate & Educational Services
136
Profile Engine
138
Mobile Operator dB
140
Subscriber dB
142
Merchant dB

Figure 14

"Virtual Card" Generation & Download



A



B

Figure 15

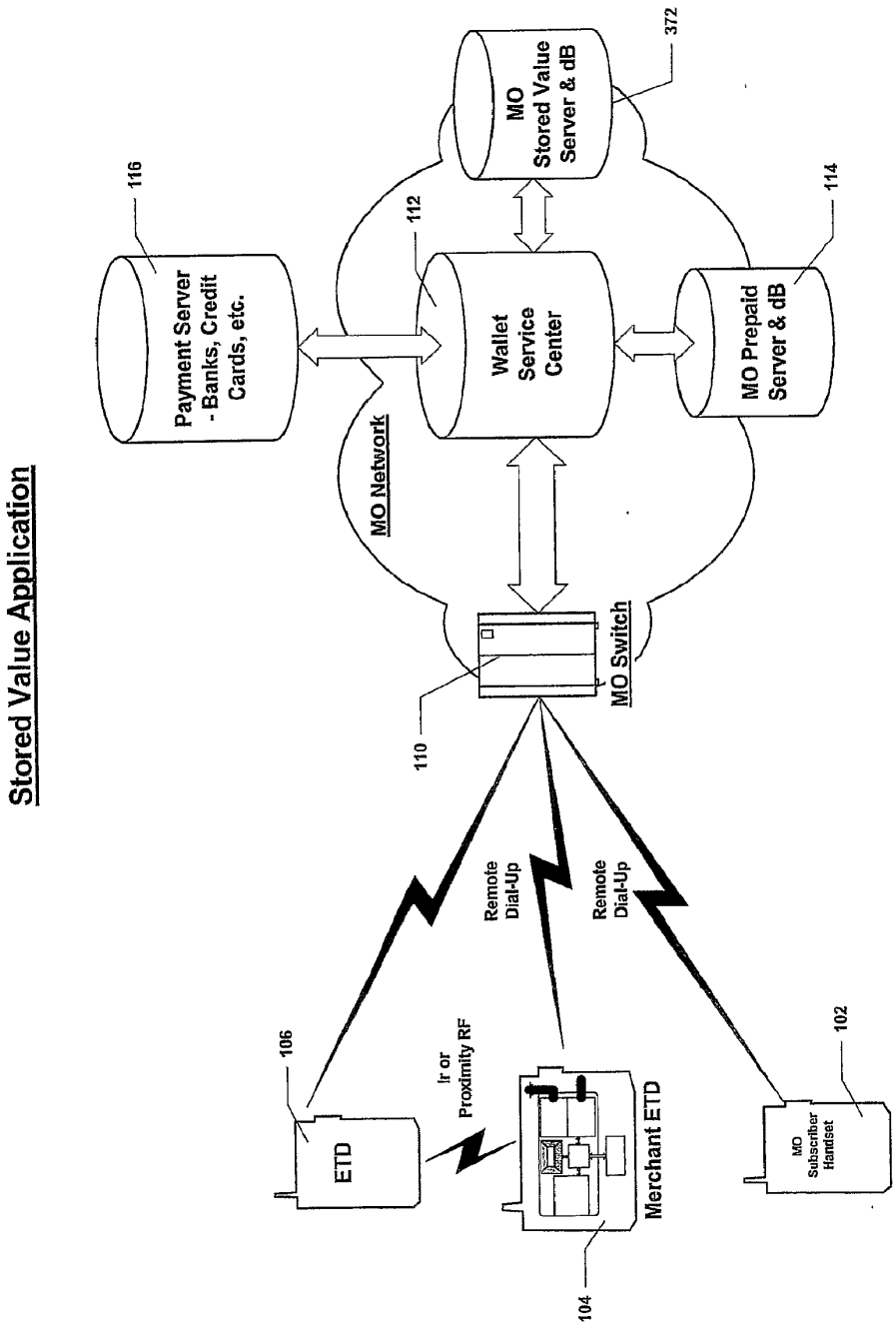

Stored Value Application
MO Stored Value Server & dB
372
116
Payment Server - Banks, Credit Cards, etc.
112
Wallet Service Center
114
MO Prepaid Server & dB
MO Network
MO Switch
110
Remote Dial-Up
Remote Dial-Up
106
Ir or Proximity RF
ETD
Merchant ETD
104
102
MO Subscriber Handset

Figure 16

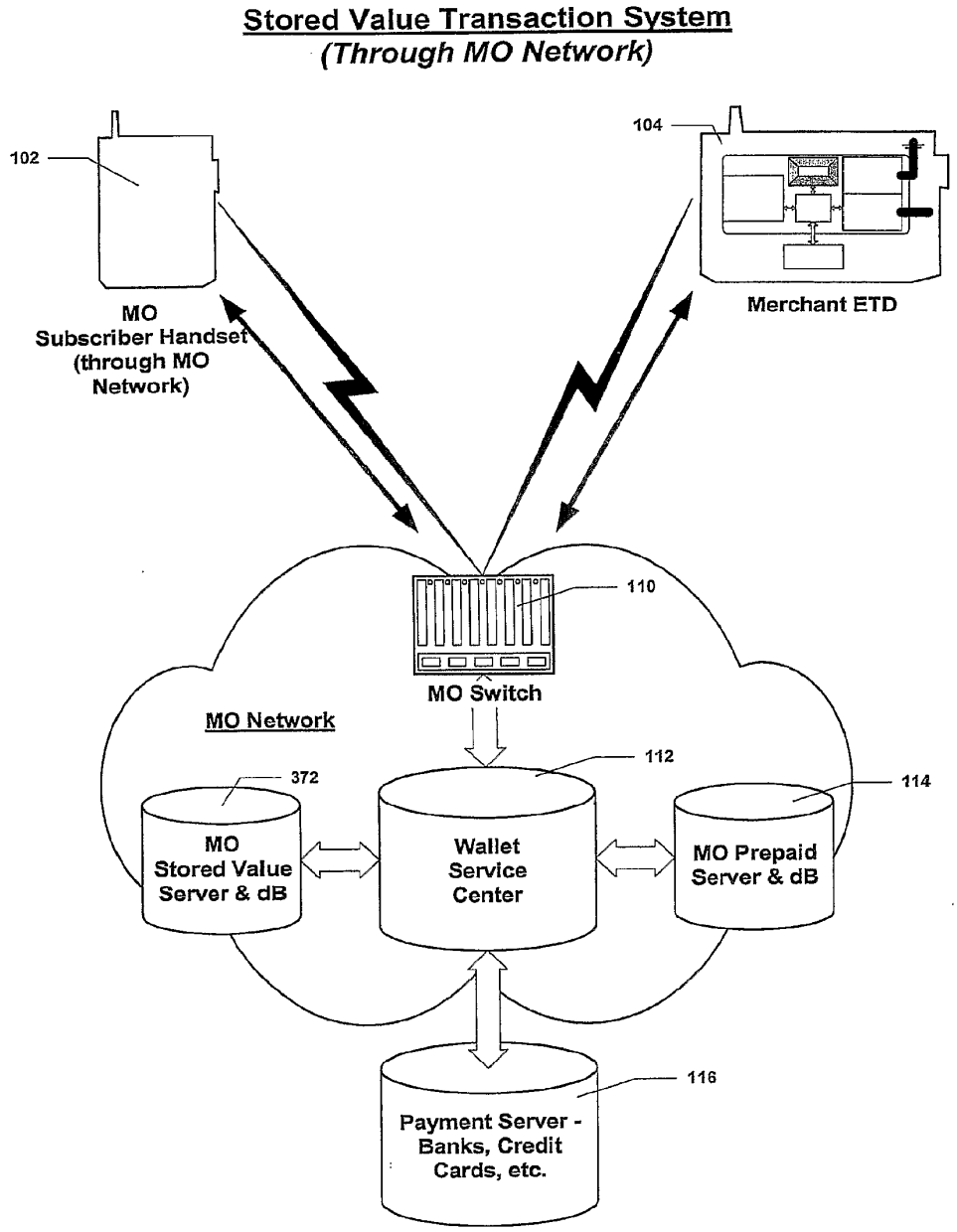

Stored Value Transaction System
(Through MO Network)
102
MO
Subscriber Handset
(through MO
Network)
104
Merchant ETD
110
MO Switch
MO Network
372
MO
Stored Value
Server & dB
112
Wallet
Service
Center
114
MO Prepaid
Server & dB
116
Payment Server -
Banks, Credit
Cards, etc.

Figure 17

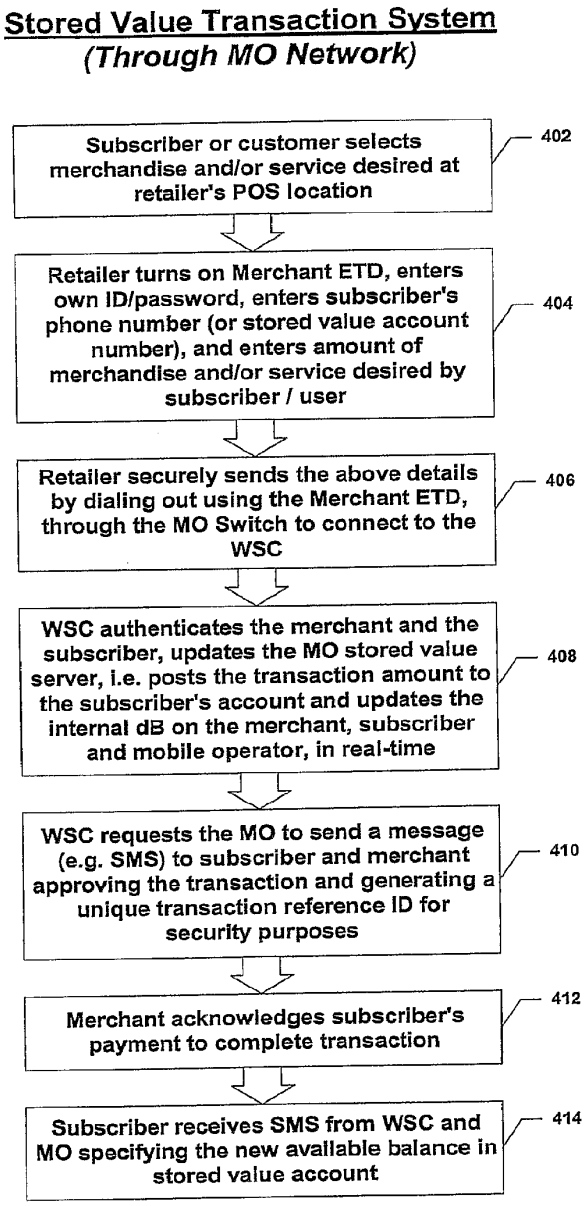

Stored Value Transaction System
(Through MO Network)
Subscriber or customer selects merchandise and/or service desired at retailer's POS location
402
Retailer turns on Merchant ETD, enters own ID/password, enters subscriber's phone number (or stored value account number), and enters amount of merchandise and/or service desired by subscriber / user
404
Retailer securely sends the above details by dialing out using the Merchant ETD, through the MO Switch to connect to the WSC
406
WSC authenticates the merchant and the subscriber, updates the MO stored value server, i.e. posts the transaction amount to the subscriber's account and updates the internal dB on the merchant, subscriber and mobile operator, in real-time
408
WSC requests the MO to send a message (e.g. SMS) to subscriber and merchant approving the transaction and generating a unique transaction reference ID for security purposes
410
Merchant acknowledges subscriber's payment to complete transaction
412
Subscriber receives SMS from WSC and MO specifying the new available balance in stored value account
414

Figure 18

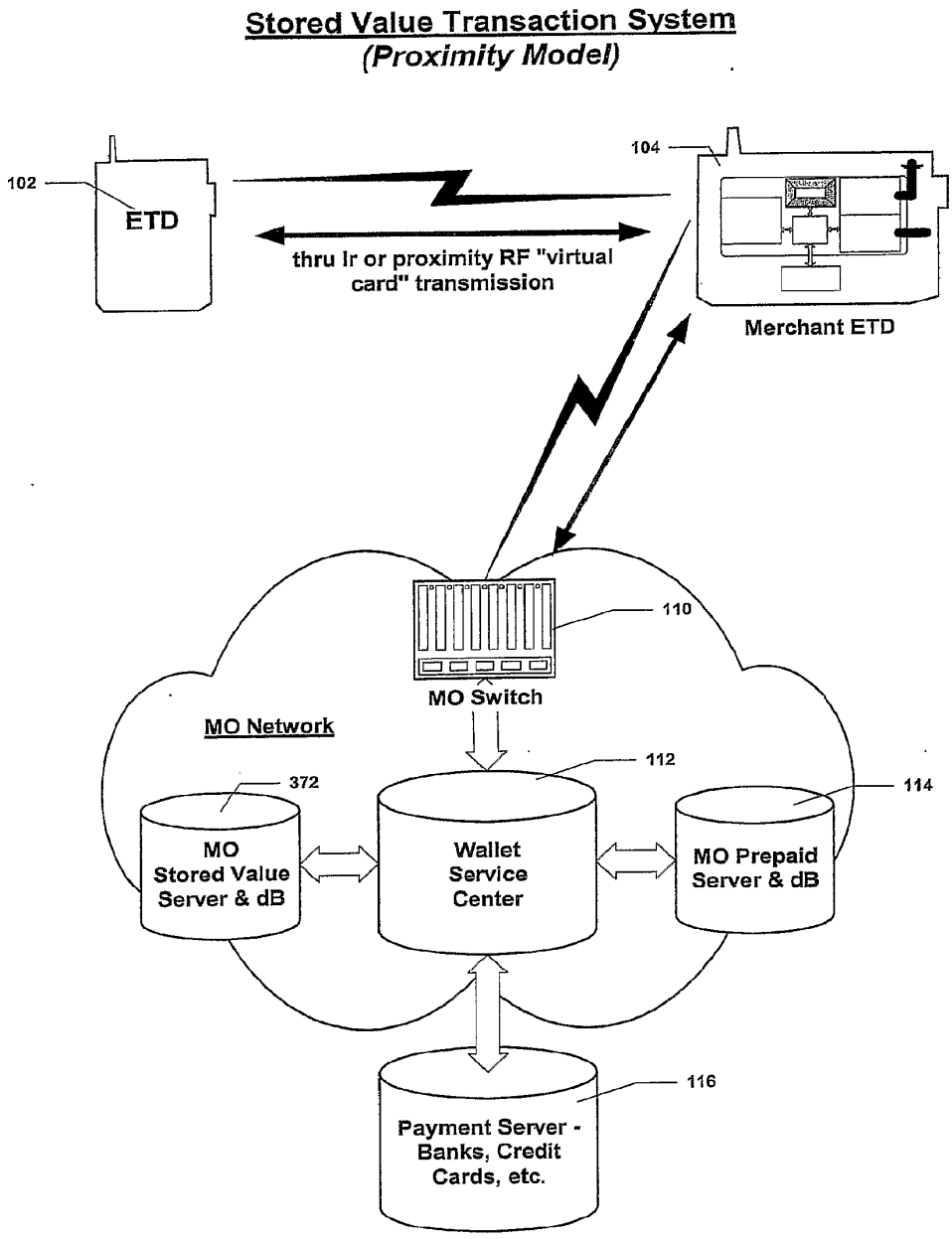

Stored Value Transaction System
(Proximity Model)
102
ETD
104
thru Ir or proximity RF "virtual card" transmission
Merchant ETD
110
MO Switch
MO Network
112
372
114
MO Stored Value Server & dB
Wallet Service Center
MO Prepaid Server & dB
116
Payment Server - Banks, Credit Cards, etc.

Figure 19

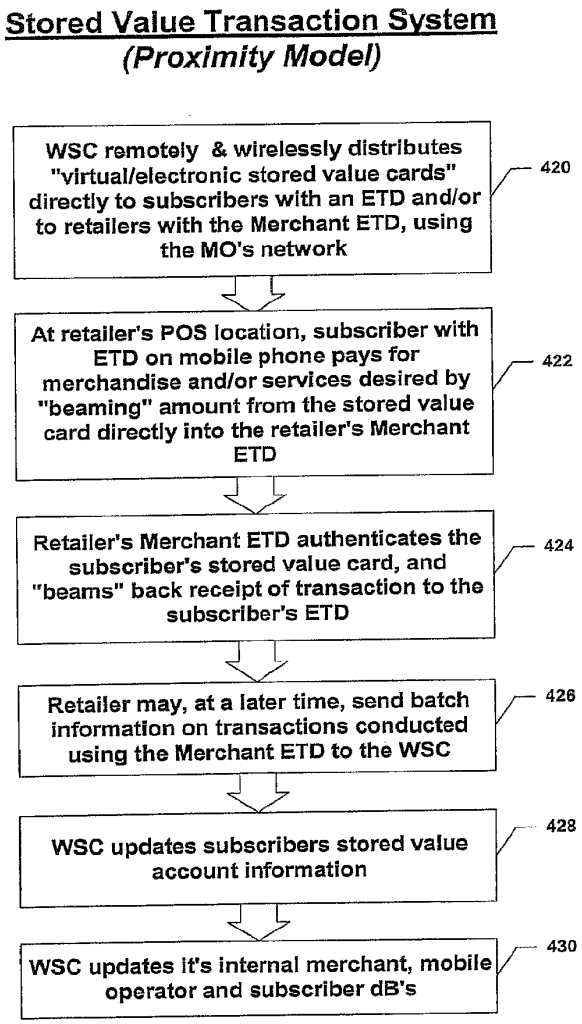

Stored Value Transaction System
(Proximity Model)
WSC remotely & wirelessly distributes "virtual/electronic stored value cards" directly to subscribers with an ETD and/or to retailers with the Merchant ETD, using the MO's network
420
At retailer's POS location, subscriber with ETD on mobile phone pays for merchandise and/or services desired by "beaming" amount from the stored value card directly into the retailer's Merchant ETD
422
Retailer's Merchant ETD authenticates the subscriber's stored value card, and "beams" back receipt of transaction to the subscriber's ETD
424
Retailer may, at a later time, send batch information on transactions conducted using the Merchant ETD to the WSC
426
WSC updates subscribers stored value account information
428
WSC updates it's internal merchant, mobile operator and subscriber dB's
430

Figure 20

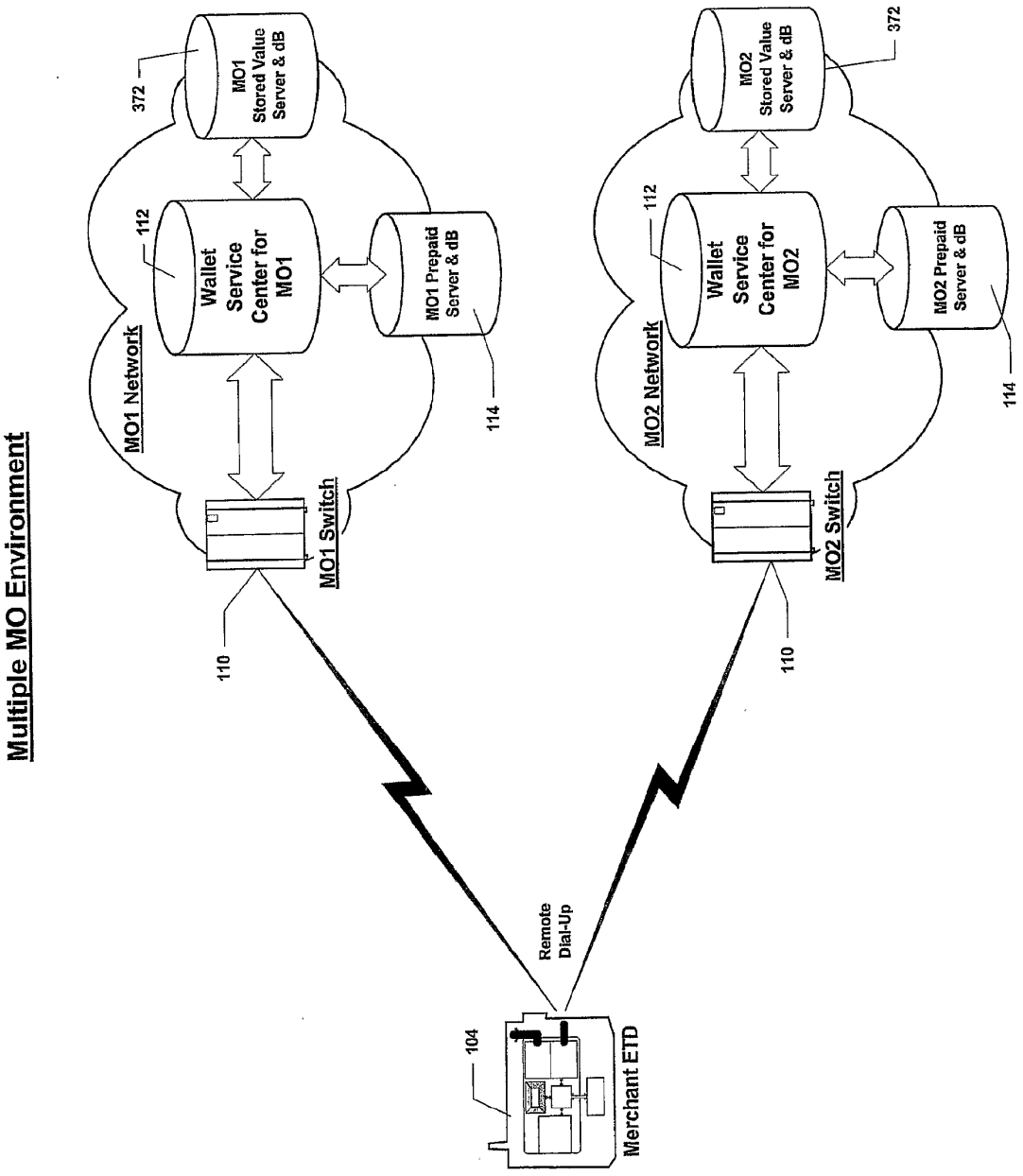

Multiple MO Environment
MO1 Network
MO1 Stored Value Server & dB
372
Wallet Service Center for MO1
112
MO1 Prepaid Server & dB
114
MO1 Switch
110
MO2 Network
MO2 Stored Value Server & dB
372
Wallet Service Center for MO2
112
MO2 Prepaid Server & dB
114
MO2 Switch
110
Remote Dial-Up
104
Merchant ETD

Figure 21

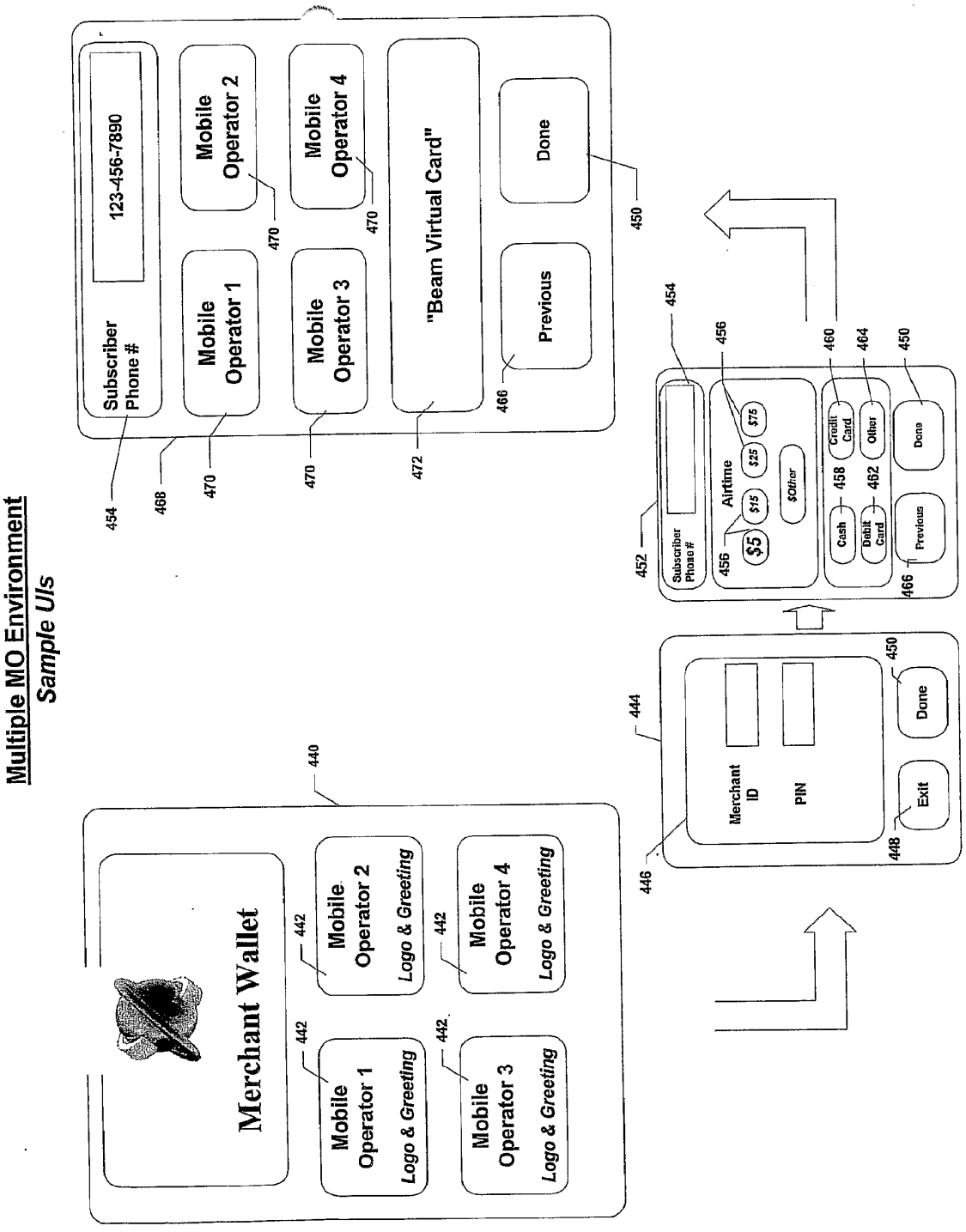

Multiple MO Environment
Sample UIs
Merchant Wallet
Mobile Operator 1
Logo & Greeting
Mobile Operator 2
Logo & Greeting
Mobile Operator 3
Logo & Greeting
Mobile Operator 4
Logo & Greeting
Subscriber Phone #
123-456-7890
Mobile Operator 1
Mobile Operator 2
Mobile Operator 3
Mobile Operator 4
"Beam Virtual Card"
Previous
Done
Merchant ID
PIN
Exit
Done
Airtime
$5
$15
$25
$75
$Other
Cash
Debit Card
Credit Card
Other
Previous
Done
440
442
444
446
448
450
452
454
456
458
460
462
464
466
468
470
472

Figure 22

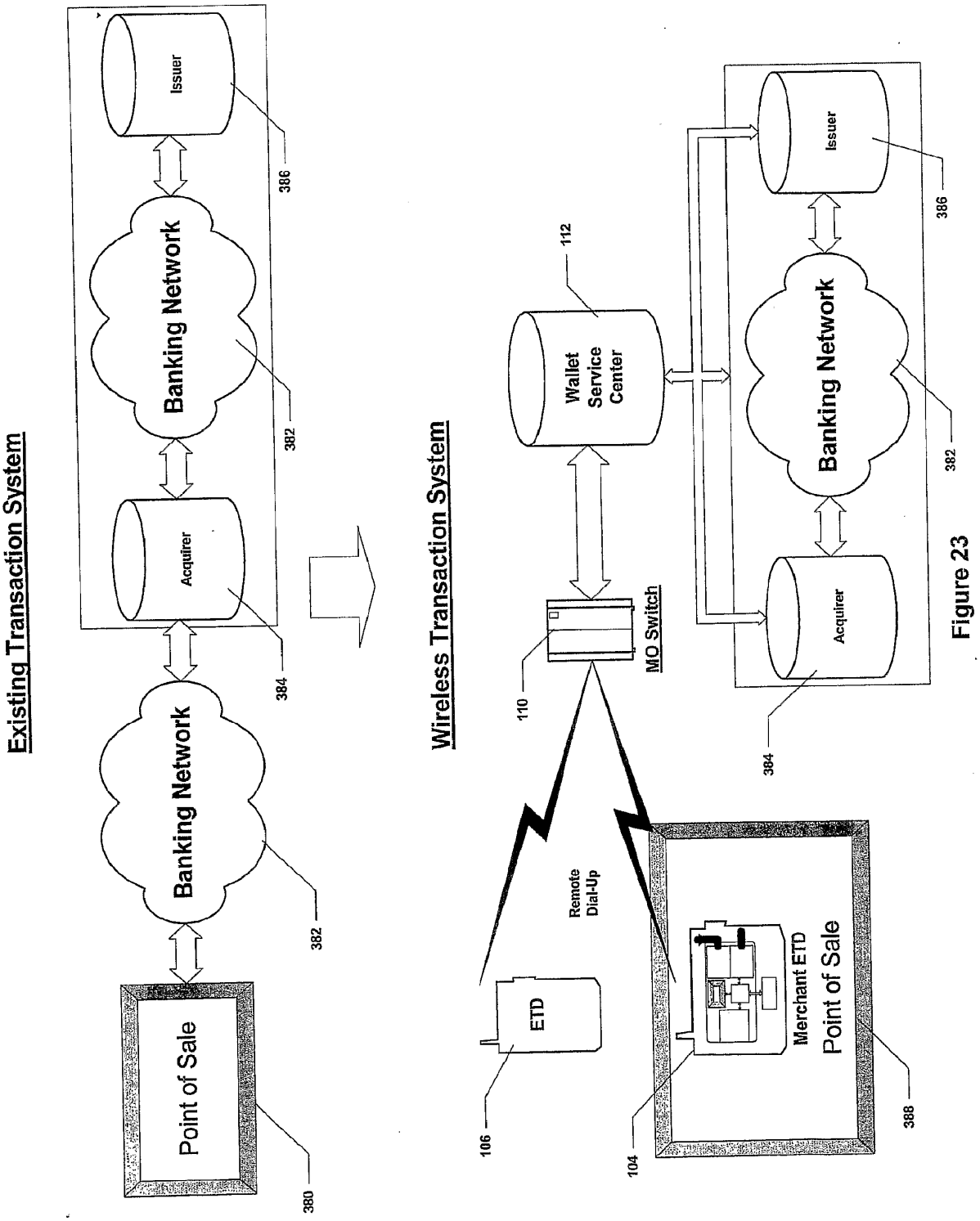

Existing Transaction System
Issuer
386
Banking Network
382
Acquirer
384
Banking Network
382
Point of Sale
380
Wireless Transaction System
112
Wallet Service Center
Issuer
386
Banking Network
382
110
MO Switch
Acquirer
384
Remote Dial-Up
ETD
106
Merchant ETD
Point of Sale
104
388

Figure 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/23899

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G 06 F 17/60
US CL :705/65

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/65, 1, 53

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, search terms: pre-paid, virtual card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 5,828,740 A (KHUC et al.) 27 October 1998, col.1 lines 11-65, col. 2, lines 25-64, col. 3, lines 1-27, col. 4, lines 8-24.	1 and 5 ---------- 2-4 and 6-17
Y	US 6,105,008 A (DAVIS et al.) 15 August 2000, col. 7, lines 24-64 and col. 8, lines 11-32.	2-4 and 8-17
Y	US 6,185,545 B1 (RESNICK et al.) 6 February 2001, FIG. 2	6 and 7

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 24 SEPTEMBER 2001	Date of mailing of the international search report 16 NOV 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer HYUNG S. SOUGH Telephone No. (703) 308-0505

Form PCT/ISA/210 (second sheet) (July 1998) ★

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010393 A1

(51) International Patent Classification[7]: G07F 19/00, H04M 17/00

(21) International Application Number: PCT/IL2002/000601

(22) International Filing Date: 21 July 2002 (21.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **PARTNER COMMUNICATIONS COMPANY LTD.** [IL/IL]; 8 Ha'amal St., Afek Industrial Park, 48103 Rosh Ha'ayin (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **FELDMAN, Avi** [IL/IL]; 8 Ha'amal St., Afek Industrial Park, 48103 Rosh Ha'ayin (IL).

(74) Agent: **CALDERON, Hana**; Jacob & Hana Calderon, Advocates, Crystal Bldg., 12 Hilazon St., 52522 Ramat Gan (IL).

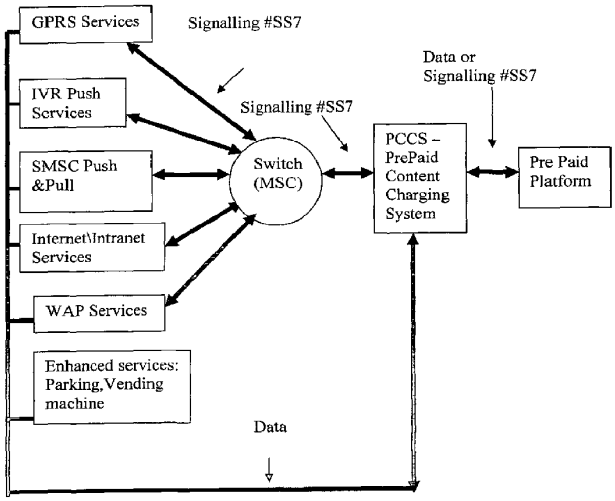
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PREPAID CHARGING SYSTEM AND METHOD



(57) Abstract: A complementary system for charging Prepaid subscribers implemented in a PLMN, PSTN or DATA communication network with a plurality of Service platforms using different #SS7 and Data communication protocols and a Prepaid platform with real time charging means that communicates through a limited number of communication protocols. The PCCS monitors the signaling and Data in the network and initiates a balance request or a charge request to the Prepaid platform when a balance or charge request is received by the PCCS following a session request from a Prepaid subscriber or the opening of a session by a push platform in the case of a push service. The prepaid platform routs an account status response or "adequate balance" or a "balance inadequate" response with or without an account status response to the PCCS which then issues a "supply service" or a "do not supply service" response to the Service Platform.

WO 2004/010393 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PREPAID CHARGING SYSTEM AND METHOD

Background of the Invention:
The so called Pre Paid service was developed with a view to supply a limited range of voice telephony services to users with a tight budget or users whose budget is controlled by others such as children under age, employees using a business telephone, prisoners etc..

According to this prevailing concept of the Prepaid Service, content services such as Data services, SMS Services, Vending machine services,GPRS services, Internet services,WAP services, IVR Enhanced Services etc. are considered out of scope. Consequently methods of charging have been developed for the voice telephony market only, the various content services remaining unsupported or not fully supported by the PrePaid platforms for the reason that these platforms are only able to monitor a limited range of # SS7 protocols and most of them are unable to monitor Data.

This attitude of the prior art to the Pre Paid service resulted in a much larger variety of services being available for the Post Paid subscriber than those enjoyed by the Pre Paid subscriber, the reason being that the operator is unable to charge the Pre Paid subscribers for those services. Obviously the present state of the art leaves a large amount of consumer demand unattended. The more so as children and teenagers, naturally belonging to the Pre Paid customer group, tend to make an extensive use of innovative and sophisticated data services.

It is a main drawback of the prior art that Pre Paid vendor systems are designed to support their own Pre Paid services only, while any other platform services are left without precharging means. Thus an Operator implementing a Pre Paid platform will not be able to supply his full variety of services to the PrePaid subscribers.

The PrePaid market has therefore created a demand for a PrePaid system with a payment method that is not limited to a class of services. It is another demand of the market that a general operator with different platforms and services be capable of supplying the same advanced voice and data services for his PrePaid subscribers and Post Paid subscribers.

It is therefore desirable to provide a PrePaid Content Charging System that enables any PrePaid Operator, regardless of the Pre Paid Platform implemented by the said Pre Paid Operator, the PrePaid services to be supplied or the kind of #SS7 or Data protocols or technology operated in the said network, to charge and support the same Content services, including Data services such as: SMS, WAP, Internet (Push and Pull forms), GRPS and Enhanced Voice Services, that are supported for the post paid subscribers.

Further, it is desirable to provide a real time charging mechanism for a Content Service such that the PrePaid subscriber is charged in the course of ordering or immediately after getting the desired service, according to any marketing definitions.

Summary of the Invention

The invention concerns a charging system that is applicable in cellular telephony systems or wired systems (PSTN) or any other communication network systems using PLMN/PSTN/DATA technologies and that enables real time charging of PrePaid subscribers for various Data and Voice services including Content services and Advanced Voice services employing a variety of Data and # SS7 protocols, regardless of the type of the PrePaid platform, network platform or service platforms applied in the said communication sytem.

The inventive PrePaid Content Charging System (hereafter - PCCS) is designed to function as a charging request gateway or as a service junction which includes the PrePaid subscribers Database. The PCCS monitors the different kinds of # SS7 signalling or Data in the network and it enables real time charging of the Pre Paid subscriber by routing a balance request or a charge request to the PrePaid platform via #SS7 signaling that is compatible with the said PrePaid platform when a service request or a charging request has been routed to the PCCS by a service platform via any of the said different #SS7 or Data signalling as a result of a session initiated by a PrePaid subscriber. All PrePaid subscribers related service requests are balance analyzed and charged accordingly by the PrePaid Platform that sends a response of "balance adequate" or "balance inadequate" or account status to the PCCS whereupon the PCCS responds accordingly by putting out a "supply service" or "deny service" response to the relevant service platform, via #SS7 or Data signalling appropriate for that platform.

In the event of a "push" service, the balance request or charge request is routed to the PCCs by a relevant "push" platform when the time that has been set for the service by the prepaid user arrives. In case that there is a finding of "balance inadequate", the PCCS repeats the "balance request" or "charge request" a preset number of times until a balance adequate response is received.

In accordance with another aspect of the invention, the PCCS may also comprise means for managing and supplying one or more PrePaid related services such as Vending machine, Parking machine, etc.

The inventive PCCS enables charging a PrePaid subscriber for any services in the network such as Push and Pull SMS services, Internet, Intranet,WAP, push IVR services, enhanced services such as Parking,Vending machines etc.

Brief Description of the Drawings

Fig. 1 is a schematic representation of the PrePaid platform connections in an existing cellular network.
Fig. 2 is a schematic representation of the charging process in an existing network
Fig. 3 is a schematic representation of the PCCS network connections
Fig. 4 is a block diagram of a Network in which a PCCS system is implemented
Fig. 5 is a representation of the charging call flow for push or pull services in a network with a PCCS system
Fig. 6 is a schematic representation of the basic architecture of a PCCS system

Detailed Description of the Invention in Respect of a Preferred Embodiment

Cellular telephony services providers cater to Post Paid as well as Pre Paid users. While the Post Paid user gets the desired service on the basis of future charging, the Pre Paid user may only use the service on the condition that his balance has been checked and found sufficient for the requested operation. It is therefore necessary to monitor the balance of the PrePaid user, to consider it before supplying the service, to make the decision of supplying or denying the service in real time, to charge the Customer for the service instantly and to continue monitoring the service during use such that it may be terminated when the customer reaches balance inadequate.

Current charging methods in the PrePaid World are of two kinds. The Real Time Charging method involves a PrePaid Data Base and charges Voice calls according to the PrePaid Calling Numbers, some PrePaid platforms also supporting Mobile Originated SMS and Terminated Called Numbers, whereas according to the Calling Detail Record (CDR) based Charging method – only PrePaid CDRs are analyzed and the PrePaid subscriber balance is charged accordingly.

A schematic representation of the PrePaid platform connections in an existing cellular network is shown in Fig. 1. As seen in Fig. 1, when a service is required by a Prepaid user, the Prepaid user's mobile handset initiates a request to a Mobile Switching Center (MSC) using # SS7 protocol which then sends a request to the Prepaid platform also via # SS7 protocol, the Prepaid platform response indicating via # SS7 protocol whether the subscriber's account allows him to receive the specific service. Where the response is positive, the Mobile Switching Center connects the subscriber to the requested service. In the network of Fig. 1, the PrePaid platform is only capable of performing the above described authorizing procedure in respect of Short Message Service Center (SMSC) and Mobile Originated (MO) services such as Voice Calls and Mobile Originated SMS while many other services such as SMS Push services, IVR Push Services, WAP, GPRS as well as Internet/intranet services remain out of scope for the PrePaid user for the reason that the PrePaid platform is incapable of monitoring the types of #SS7 or Data protocols employed for these services. Many PrePaid platforms fail to support even mobile originated SMS services, while other PrePaid platforms may be suited to support different types of services such as IVR only, WAP only etc., all according to PrePaid platform design. While in Fig. 1 a cellular network with a Mobile Switching Center is described, it will be understood that other Switching Center means may be used for different communication networks as known.

It will be understood that the considerably limited scope of current Prepaid Charging systems results in a large number of services being blocked for PrePaid subscribers in systems of the known type, the kind of services blocked depending on the kinds of #SS7 protocols compatible with the said PrePaid Charging system as a result of Designer choice.

While CDR based charging may be applied for services that are not supported by the PrePaid platform, this charging method has the drawback of not enabling any real time charging. This means that the operator may fail to charge the service, resulting in loss of valuable income.

The charging of Content Services in existing Prepaid Charging platforms is related to the capabilities of the PrePaid platform vendor and not to the services to be charged. In other words, the PrePaid platform is only capable of charging for a limited number of services according to its design while other platform services cannot be supplied to PrePaid users due to lack of charging means.

Fig. 2 shows the charging flow of a voice session in an existing network comprising a PrePaid Platform and a Switching Center such as the network of Fig. 1, the said charging flow comprising the following steps:

Step 1: The Prepaid subscriber initiates the session by calling a destination and/or requesting a service

Step 2: The Switching Center initiates a balance request or a charging request to the PrePaid platform

Step 3: The PrePaid platform responds according to the subscriber balance: in case that the balance is adequate, a "connect" response is routed to the Switching Center, otherwise the response routed to the Switching Center is "disconnect".

Step 4: in the event of an adequate balance the call will be routed by the Switching Center to the Called Party and it will be charged accordingly by the Prepaid platform .

In the event of an inadequate balance the call will not be routed. In some systems an announcement of "balance too low" is displayed or played to the PrePaid subscriber.

It will be understood that in some cases the PrePaid subscriber may also be the Called party, such as in the case where a third party requests a service that involves a call to the Prepaid subscriber.

In the case of a Service session, where the balance is adequate the call will be routed to the requested Service platform. However this operation is only feasible where the PrePaid platform is capable of using the type of $SS7 or Data protocol of the respective Service platform.

It is a main drawback of the prior art that due to the existing PrePaid platforms being incompatible with the protocols implemented in most services and technologies available on cellular and PSTN networks, the above described charging flow can only be realized with respect to a very limited number of services .

While the drawings of Figs. 1 and 2 refer to a cellular network, it will be understood that PrePaid subscribers in PSTN (wired) networks are subject to similar drawbacks and therefore it is also desirable to enable the charging of various additional services for the PrePaid PSTN subscriber.

The PrePaid market charging requirements demand that Content Services be charged regardless of the PrePaid platform vendor and PrePaid platform version. It is a further demand of the market that Content services be charged, regardless of the type of service or service platform (WAP, IVR, Internet or other) and regardless of the type of #SS7 or Data protocol used by a service or service platform and that Pre Paid subscribers be charged regardless of service technology, whether GSM, GPRS, CDMA, TDMA or other. The Pre Paid market demands a very fast introducing and charging of newly launched Content Services to the Pre Paid subscriber.

In accordance with the present invention a Pre Paid Content Charging System (PCCS) is proposed that enables the implementing of a real time method for the charging of PrePaid subscribers in respect of a large variety of services, platforms and technologies, including Content services and advanced Voice services.

The invention will be described hereinbelow by way of example in respect of a preferred embodiment. It will be understood however that many other variations and modifications of the invention may be made that still remain within the scope of the description and the claims.

In accordance with the invention the PCCS is implemented in a telephony network with a Prepaid Platform that may be a PSTN (Public Switching Telephony Network) or PLMN (Public Land mobile Network) or any other communication network type, and it monitors the signalling or the Data in the said network. The PCCS is provided with means for monitoring the network signalling according to a variety of # SS7 protocols such as Wireless Application Protocol (WAP), IN Application Protocol (INAP), or ISDN User Part Protocol (ISUP) or any other #SS7 protools applied in the network. The PCCS is further provided with means for monitoring the network Data using a variety of Data protocols such as HTTP/TCP/IP, HTTP/UCP, HTTP/MAP or any other Data Protocol applied in the network. The PCCS further has means for communicating with the PrePaid platform.

Signalling or Data in the Network that constitutes a PrePaid call or message is analyzed according to a PrePaid customer database such that all PrePaid subscribers related service requests are balance analyzed and charged accordingly.

The PCCS may be implemented as a charging request gateway or it may be implemented as a service junction that comprises the PrePaid subscribers Database.

Within the network the PCCS is connected to a BSCS (Business Support and Control System), BGW (Billing Gateway) and SOG (Service Order Gateway) or any similar subscriber management means in order to allow management of the PrePaid subscribers.

The PCCS enables the charging of a PrePaid subscriber for various services in the network supplied by platforms of various types such as Push and Pull SMS, Internet, Intranet,WAP, push IVR services, enhanced services such as Parking,Vending machines etc.

Fig. 3 is a schematic representation of a network in which the PCCS of the invention is applied, showing the PCCS connections in the network. As shown in Fig. 3, the PCCS connections may comprise a DWH (Data Warehouse) means for storing and processing subscriber CDRs, a BGW (Billing Gateway) means for processing raw CDRs from network platforms, a SOG (Service Order Gateway) means for storing subscriber characteristics, a BSCS (Business Support and Control System) means for storing a subscriber database, and a CSR (Customer Service Representative) such that managing and controlling customer service and data is facilitated. It will be understood by those versed in the art that the above listed systems communicate via Data protocols. Other PCCS connections comprise a variety of services and platforms that are available in the network such as IVR, GPRS,WAP, using various #SS7 protocols and SMSC, IN and Internet Gateway means using Data protocols of different kinds. In accordance with the invention, all of the above listed services may be supplied to a PrePaid user and charged accordingly due to the inventive PCCS having means for communicating via the said #SS7 and Data protocols.

It will be understood that a Gateway shown in Fig. 3 may also be a server and that many other services may be added in the said network to be charged by the inventive PCCS whether those existing today or any services to be developed in the future.

As seen in Fig. 3, the inventive Prepaid Charging Complementary System is connected to a PrePaid platform, the said connection enabling the PCCS to send a charging request or a balance request to the said PrePaid platform and to receive a response from the PrePaid platform. As shown in Fig. 3, the Prepaid Charging Complementary System communicates with the PrePaid Platform via #SS7 or Data protocols.

It will be understood to those versed in the art that the Prepaid Platform may be implemented as a PrePaid SCP or SDP or Prepaid Switch.

In Fig. 3 some of the different protocols that may be used for communication of the Prepaid Charging Complementary System of the invention with various systems within the network are indicated such as INAP, ISUP #SS7 protocols or TCP/IP Data protocols for communication with the PrePaid subscriber management means, TCP/IP or HTTP Data protocols for communication with the Data Warehouse means, INAP or HTTP Data protocols for communicating with IN means, HTTP or UCP Data protocols for communicating with SMSC means, HTTP or TCP/IP Data protocols for communicating with IVR service means, HTTP or MAP Data protocols for communicating with WAP gateway means and #SS7 Protocols for communicating with the Switching Center means and the GPRS Gateway means.

In accordance with a further advantage of the invention, the Prepaid Charging Complementary System may be adapted for communication via other protocols in case that such protocols are developed or applied in the future in communication networks.

It is one of the advantages of the inventive PCCS that it may be implemented in a preexisting network that comprises all or a part of the systems described in refence to Fig. 3 whereby the said network acquires the ability of supplying additional voice and data services that could not be supplied to the PrePaid subscriber prior to the installation of the said Prepaid Charging Complementary System.

Fig. 4 is a general diagram of the preferred embodiment showing a network with a PCCS, a PrePaid platform, an MSC (Mobile Switching Center) and a variety of service platforms. The MSC (Mobile Switching Center) receives the calls initiated by the subscribers via the different platforms by means of #SS7 signaling. In the event that the subscriber is a PrePaid subscriber, the Mobile Switching Center communicates with the Prepaid Charging Complementary System of the invention by initiating a service request. The Prepaid Charging Complementary System routs a balance request or a charge request to the PrePaid platform and the said PrePaid platform responds by data or signaling or both that indicates the PrePaid subscriber balance or new balance after charging of the PrePaid subscriber balance.

In the preferred embodiment, service requests may also be routed from the platforms to the PCCS directly, without passing the Switching Center means. As seen in Fig. 4, the GPRS, IVR, SMSC, Internet/Intranet and WAP service platforms communicate with the PCCS both directly and indirectly, via the MSC, while service requests from some enhanced service platforms such as Parking, Vending machines etc. are only directly routed from these platforms to the PCCS. The communication protocols used for routing the service requests include #SS7 signaling such as INAP, ISUP, MAP, UCP, CAMEL PH 2/3 and Data signaling such as HTTP, TCP/IP or any other protocol that is appropriate for the relevant service platform.

Having received a response from the PrePaid platform that indicates the said PrePaid subscriber balance, the Prepaid Charging Complementary System Signals to the relevant Service platform via INAP, ISUP, MAP, UCP, or CAMEL, PH2/3 HTTP, TCP/IP or any other #SS7 or Data protocol as appropriate depending on the relevant platform protocol and indicates a balance response according to which the service is allowed or denied.

In case of balance 0 or inadequate balance or any other predefined balance value, a "balance 0" or "balance inadequate" or any similar message is sent to the PrePaid Caller from the relevant platform, indicating that the requested service is unavailable. In accordance with the invention, the balance message may be sent by way of announcement or SMS.

In accordance with the invention, where the balance is sufficient, the charging procedure is executed by the Prepaid platform via an IN session, ISUP session or Data session in compliance with the network operational characteristics.

In accordance with another aspect of the inventive PCCS system in the event of a no acknowledge message from the PrePaid platform regarding the supply of the required service to the PrePaid subscriber, the request is repeatedly resent by the PCCS to the PrePaid platform at a later point of time until a "balance adequate" message is received by the PCCS. It will be understood that this feature of the invention has the advantage of considerably increasing the number of service events that, inter alia, by enabling Push services to Prepaid subscribers whereby the profitability of the network in which the PCCS is implemented becomes much higher.

In accordance with yet another aspect of the invention a resend service threshold is defined such that above the said threshold the service resend is ceased.

It will be understood that other service platforms, using other protocols, may be implemented in a network according to the invention and the supply of services to PrePaid users by these platforms may be managed by employing the inventive PCCS.

Fig. 5 is a more detailed presentation of the flow of various Push and Pull services in the network of Fig 4, wherein Push services are delayed services supplied at a predetermined point of time or at a point of time that is chosen by the user, the said point of time being subsequent to the call requesting the service.

As shown in Fig. 5, a balance or charge request, indicated by arrow 1', may be routed directly from the Push platform to the Prepaid Charging Complementary System. The Prepaid Charging Complementary System then initiates a balance or a charge request, indicated by arrow 3, to the Prepaid Platform. The Prepaid platform responds by sending a response designated by arrow 4 to the Prepaid Charging Complementary System, wherein the said response 4 may be an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response. The Prepaid Charging Complementary System then outputs a "supply service" or "do not supply service" signal, indicated by arrow 5', that is routed directly from the Prepaid Charging Complementary System to the relevant service platform.

In the preferred embodiment, such direct routing of a balance of charge request occurs in the case of Vending machine and similar services. It will be understood however that other modes of making the invention may be designed in which other services will be charged by routing balance or charge requests via a Switching Center means while all or some of the services that in the preferred embodiment are requested via the Switching Center means may be charged such that the respective balance or charge requests are routed directly to the Prepaid Charging Complementary System.

In accordance with another aspect of the invention, in the case of services such as IVR, WEB or SMSC, when the time chosen by the PrePaid subscriber for receiving the service arrives, the relevant Push platform initiates a request that is routed to the Prepaid Charging Complementary System via the Switching Center Means. This request is indicated by arrows 1 and 2. The Prepaid Charging Complementary System then initiates a balance or a charge request, indicated by arrow 3, to the Prepaid Platform. The Prepaid platform then sends a response indicated by arrow 4 to the Prepaid Charging Complementary System, wherein the said response 4 may be an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response. The PCCS outputs a signal to the Switching Center means designated by arrow 5 or it outputs a signal directly to the Push Platform, designated 5', the said signal being a "supply service" signal or a "do not supply service" signal according to the input 4 from the Prepaid Platform.

It will be understood that in the case of Push and Pull services that are routed through the Switching Center means, the services may be defined in a database that is comprised in the said Switching Center Means or in an external data base or they may be defined in the PCCS for the purpose of managing the said Push and Pull services.

In the case of Push and Pull services that are directly routed to the Prepaid Charging Complementary System, the said Push and Pull services are managed by an external data base or a Data base in the PCCS.

While the drawings of Figs. 4-5 refer to a cellular network, it will be understood that the inventive PCCS may also be applied in a PSTN (wired) network to enable the charging of various additional services for the PrePaid PSTN subscriber.

Fig. 6 shows the basic architecture of the PCCS of the invention. The PCCS comprises three structural levels, a Service Level, an Application level and an Interface level. The Service level comprises means for connecting to the Prepaid platform and communicating with the said Prepaid platform through an interface using #SS7 and Data protocols.
In accordance with a preferred embodiment the Service level further comprises means for managing and supplying one or more PrePaid related services such as Vending machine, Parking machine, etc.
The Application level comprises means for monitoring the incoming #SS7 signaling or Data transferred from the Interface level.
The Interface level comprises signaling and data stacks means for communication between the operator Network and the PCCS, the said signaling means using #SS7 protocols and the said data stacks means using DATA protocols that are compatible with the different services –Prepaid or Post paid – supplied in the network, whether of the PLMN or PSTN type, in which the PCCS is implemented.

It is a considerable advantage of the invention that due to the capability of the PCCS to communicate with the different elements of the network, including the PrePaid platform, the diverse service platforms and the MSC, via standard protocols, the charging operation is implemented through the most reliable and adequate method for the PrePaid platform and the services, regardless of the type of platforms applied for the various services in the network.

In accordance with another advantage of the invention, the inventive approach of the PCCS enables the merging of voice and data services with the PrePaid charging methods, allowing the operator (PSTN or PLMN) to charge a PrePaid subscriber regardless of the type of Network vendor, Content platform vendor, services or service platforms.

It is yet another advantage of the invention that the PCCS installation and activation is very simple and fast such that an old Prepaid platform may be upgraded with new Services from other vendors by installing the PCCS of the invention in a network with a Prepaid Platform of the prior art.

Claims:

1. A PrePaid subscriber charging system to be implemented in a communication network, the said communication network comprising a plurality of Service platforms using different communication protocols and a PrePaid platform with real time charging means, the said PrePaid platform being adapted to communicating with only a limited number of the said Service platforms, the said PrePaid subscriber charging system comprising a) a Service level with means for communicating with the said PrePaid platform, b) an Interface level comprising signaling and data stacks means for communication between the said communication network and the said PrePaid subscriber charging system and c) an Application level with means for monitoring signaling or data transferred from the said Interface level using the said different communication protocols, whereby the said PrePaid subscriber charging system enables real time charging of PrePaid subscribers in respect of the said plurality of Service platforms.

2. A PrePaid subscriber charging system according to claim 1 wherein the said Service level also comprises means for managing and supplying one or more Prepaid services.
3. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system is a public switching telephony network.
4. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system is a public land mobile network.
5. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said Prepaid platform is a Prepaid SCP or Prepaid switch.
6. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication system further comprises a switching center means and balance requests or charging requests from one or more of the said Service platforms are routed to the said PrePaid subscriber charging system through the said switching center means.
7. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication protocols are standard #SS7 or Data protocols.
8. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said communication protocols comprise a wireless application protocol (WAP) or IN application protocol (INAP) or ISDN user part protocol (ISUP) or HTTP or TCP/IP protocol or HTTP/UCP or HTTP/MAP protocol or any other suitable communication protocol.
9. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise an IVR push service platform or SMSC push and pull platform or Internet platform or Intranet platform or WAP services platform or Parking or Vending machine or any other suitable service platform.

10. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise a content service platform.
11. A Prepaid subscriber charging system to be implemented in a communication network according to claim 1 hereinabove wherein the said service platforms comprise an advanced voice service platform.
12. A PrePaid subscriber charging method to be implemented in a communication system according to any of the preceding claims, the said method comprising the following steps:
    a. A PrePaid subscriber initiates a session by routing a request to a Service Platform,
    b. The Service Platform routs a service request to the PrePaid subscriber charging system, using a communication protocol designed for the said Service Platform,
    c. The PrePaid subscriber charging system initiates a balance or a charge request to the said Prepaid Platform,
    d. The prepaid platform responds by sending an account status response or an "adequate balance" or a "balance inadequate" response with or without an account status response to the said PrePaid subscriber charging system,
    e. The said PrePaid subscriber charging system outputs a signal of supply service or do not supply service to the said service platform according to the said response from the said Prepaid Platform.
13. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said service request is routed to the said PrePaid subscriber charging system via the said switching center means.
14. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said Service platform is a Push platform and the said session is initiated by the said Push platform at a point of time that had been preset by the said Prepaid subscriber.
15. A Prepaid subscriber charging method according to claim 12 hereinabove wherein the said Service platform is a Push platform and the said session is initiated by the said Push platform at a point of time that had been preset by a third party.
16. A Prepaid subscriber charging method according to claim 2 hereinabove wherein in the event that a "balance inadequate" response is sent from the said Prepaid Platform to the said Prepaid subscriber charging system the said Prepaid subscriber charging system repeats the said balance or charge request at preset intervals until a "balance adequate" response is received or until a preset number of repeated balance or charge requests has been performed.

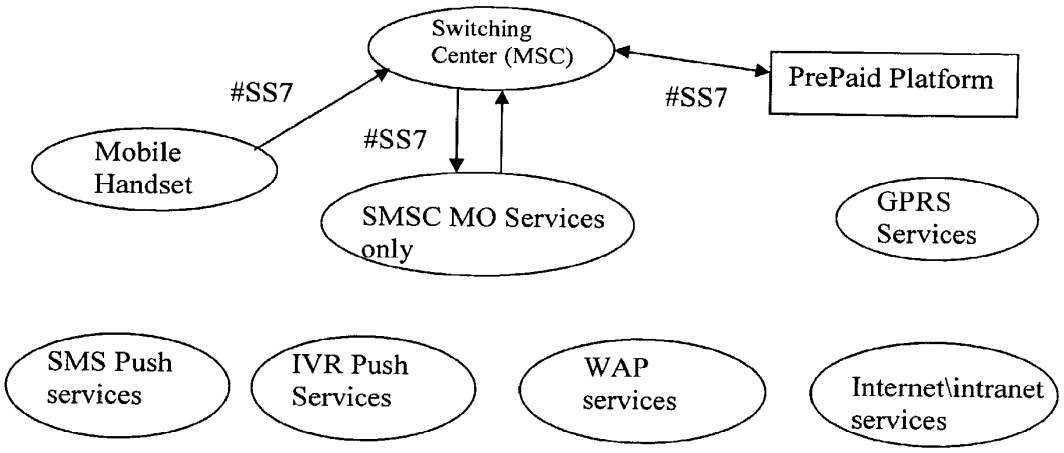

Switching Center (MSC)
PrePaid Platform
#SS7
#SS7
#SS7
Mobile Handset
SMSC MO Services only
GPRS Services
SMS Push services
IVR Push Services
WAP services
Internet\intranet services

Fig. 1

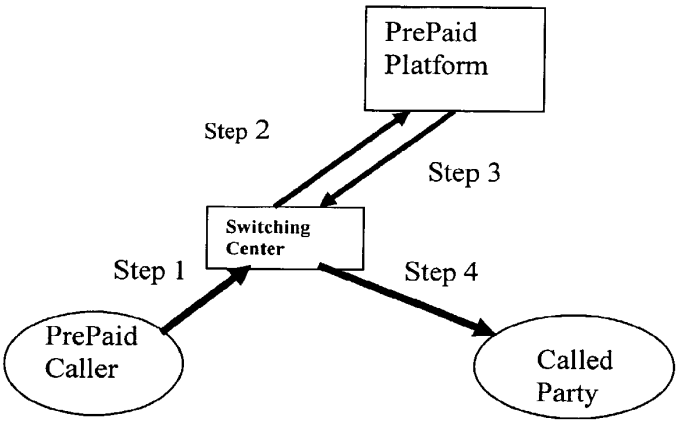

PrePaid
Platform
Step 2
Step 3
Switching
Center
Step 1
Step 4
PrePaid
Caller
Called
Party

Fig. 2

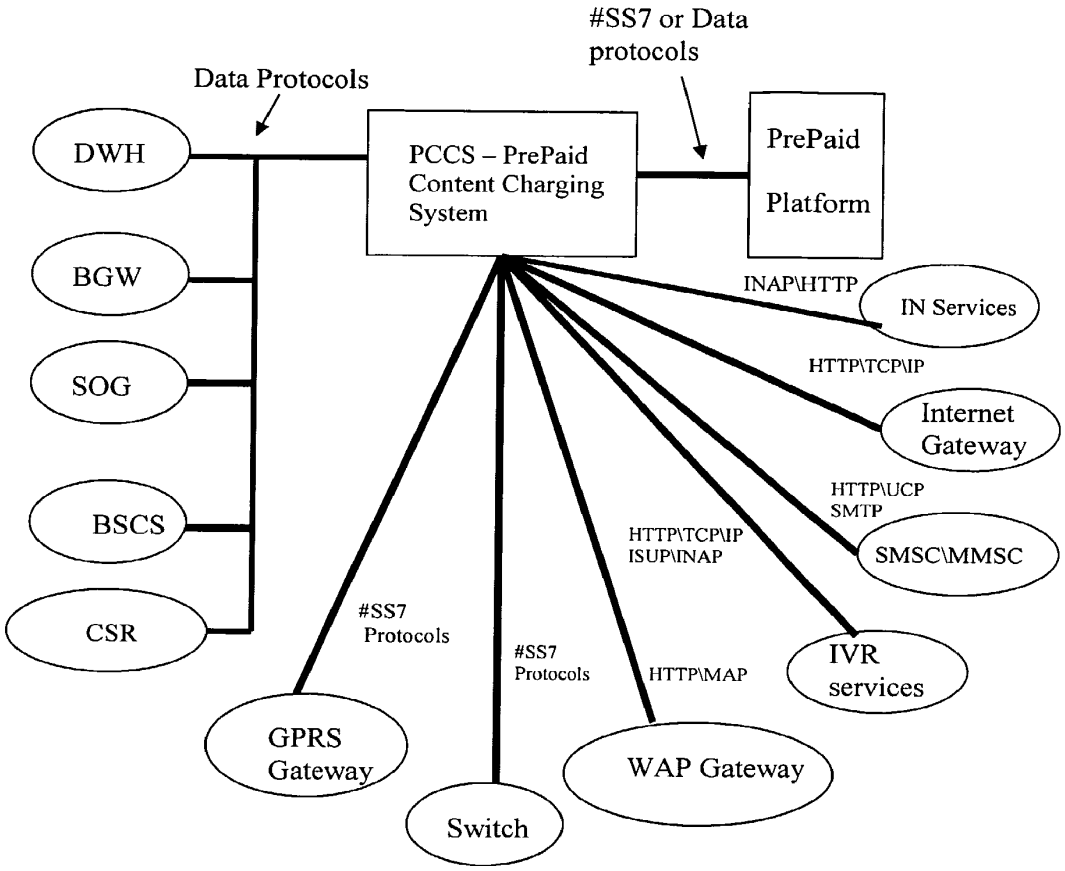

#SS7 or Data protocols
Data Protocols
DWH
BGW
SOG
BSCS
CSR
PCCS – PrePaid Content Charging System
PrePaid Platform
INAP\HTTP
IN Services
HTTP\TCP\IP
Internet Gateway
HTTP\UCP SMTP
SMSC\MMSC
HTTP\TCP\IP ISUP\INAP
IVR services
#SS7 Protocols
#SS7 Protocols
HTTP\MAP
GPRS Gateway
Switch
WAP Gateway

Fig. 3

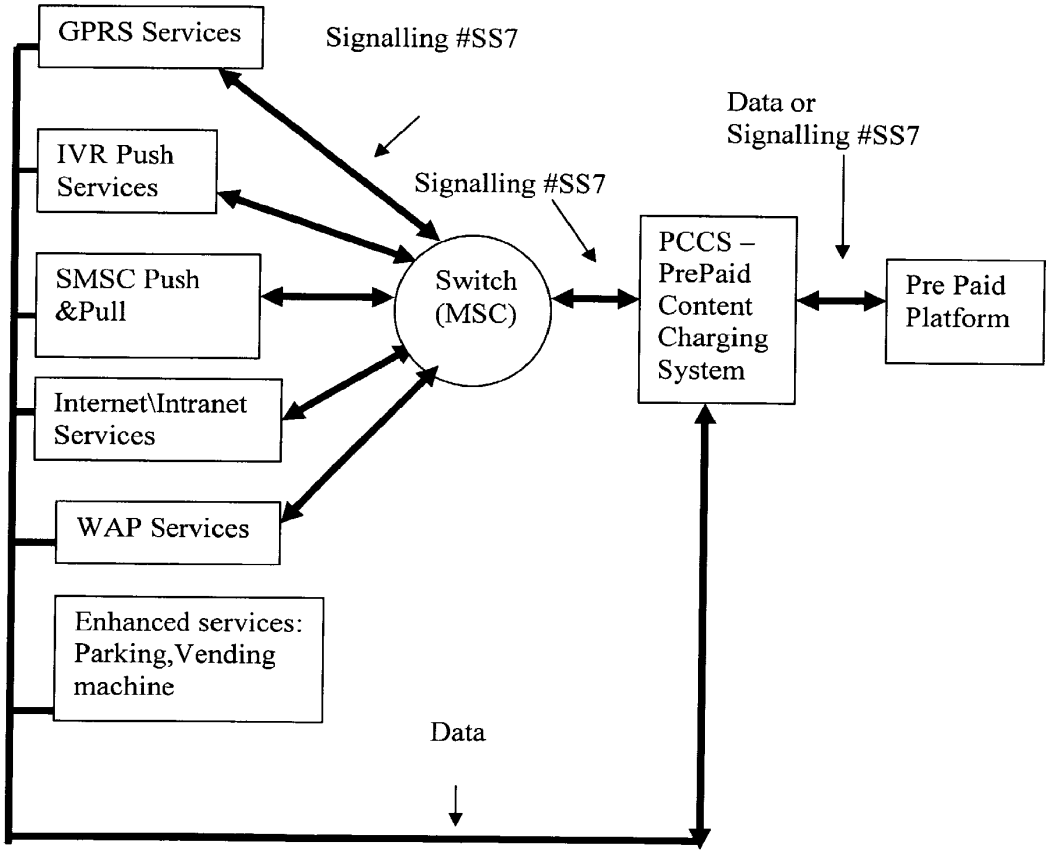

GPRS Services
Signalling #SS7
Data or
Signalling #SS7
IVR Push
Services
Signalling #SS7
SMSC Push
&Pull
Switch
(MSC)
PCCS –
PrePaid
Content
Charging
System
Pre Paid
Platform
Internet\Intranet
Services
WAP Services
Enhanced services:
Parking,Vending
machine
Data

Fig. 4

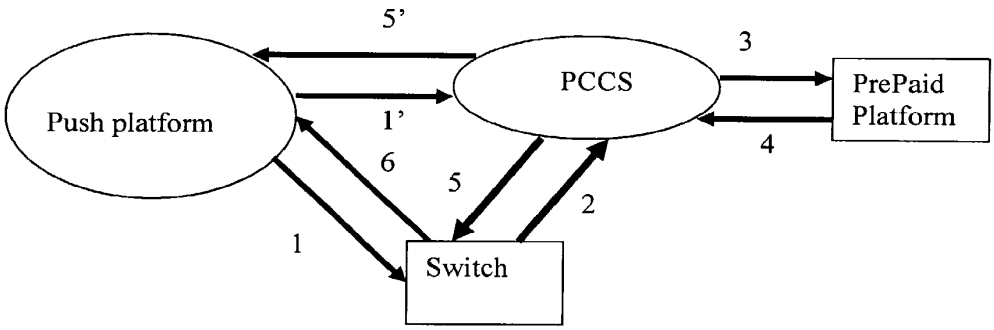


Fig. 5

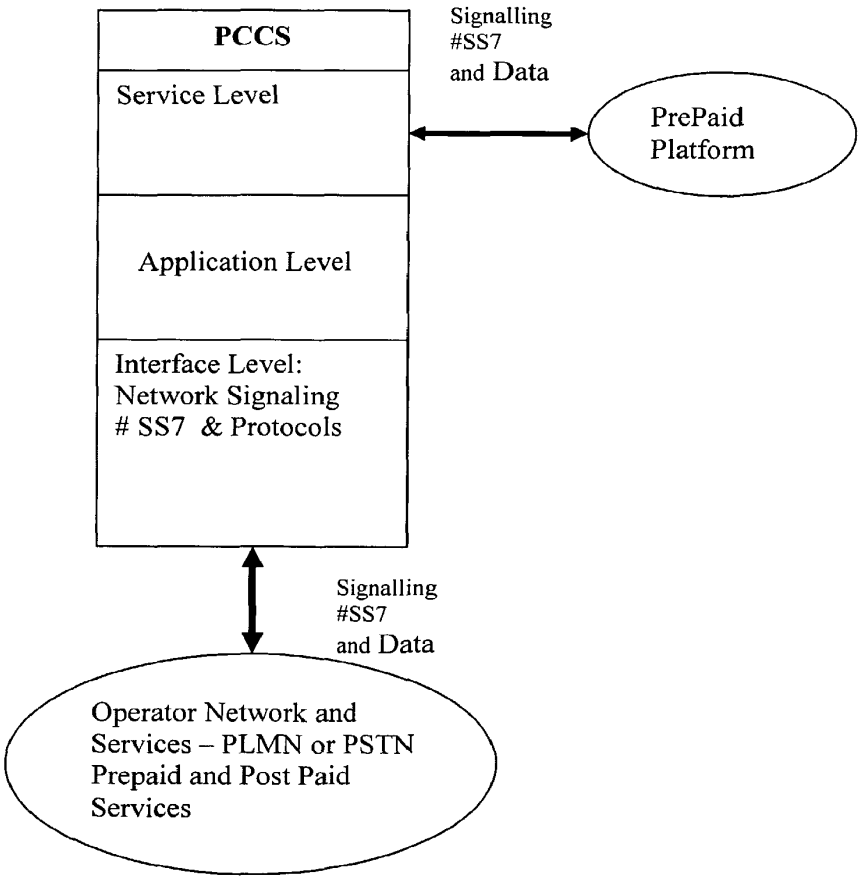

PCCS
Service Level
Application Level
Interface Level:
Network Signaling
SS7 & Protocols
Signalling
#SS7
and Data
PrePaid
Platform
Signalling
#SS7
and Data
Operator Network and
Services – PLMN or PSTN
Prepaid and Post Paid
Services

Fig. 6

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 H04M17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 825 857 A (KHALIL ANIS ET AL) 20 October 1998 (1998-10-20) figures 3,4 column 3, line 17 - line 20 column 5, line 66 -column 6, line 14 column 6, line 38 - line 54 column 7, line 58 -column 10, line 30; figures 9A-J	1,3,4, 7-9,12, 13
X	US 5 640 446 A (KULT GEORGE MICHAEL ET AL) 17 June 1997 (1997-06-17) column 2, line 30 - line 56 column 4, line 56 - line 60 column 6, line 25 - line 47 column 17, line 23 - line 43	1-3,5,7, 8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 July 2003	16/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schofield, C

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

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 93559 A (MURPHY ANNA M ;MOORE RICHARD B (US); VOGNSEN DAVID K (US); WORLDCO) 6 December 2001 (2001-12-06) page 6, line 13 -page 7, line 2 page 11, line 13 -page 12, line 3 figure 1 ---	9
A	WO 97 17678 A (NOKIA TELECOMMUNICATIONS OY ;HANNULA ANTTI (FI); KARI HANNU (FI)) 15 May 1997 (1997-05-15) page 3, line 18 - line 28 page 9, line 1 - line 29 -----	1-16

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5825857	A	20-10-1998	NONE		
US 5640446	A	17-06-1997	NONE		
WO 0193559	A	06-12-2001	AU	6530201 A	11-12-2001
			CA	2410161 A1	06-12-2001
			EP	1295461 A1	26-03-2003
			WO	0193559 A1	06-12-2001
			US	2002046255 A1	18-04-2002
WO 9717678	A	15-05-1997	FI	955354 A	08-05-1997
			AT	205002 T	15-09-2001
			AU	711112 B2	07-10-1999
			AU	7301496 A	29-05-1997
			CA	2236899 A1	15-05-1997
			CN	1203680 A ,B	30-12-1998
			DE	69614873 D1	04-10-2001
			DE	69614873 T2	11-04-2002
			EP	0865641 A1	23-09-1998
			ES	2160841 T3	16-11-2001
			WO	9717678 A1	15-05-1997
			HK	1016306 A1	12-04-2002
			JP	2000500256 T	11-01-2000
			US	2001011256 A1	02-08-2001

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023353 A1

(51) International Patent Classification[7]: G06F 17/60, 153/00

(21) International Application Number:
PCT/AU2003/001126

(22) International Filing Date:
3 September 2003 (03.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002951198 3 September 2002 (03.09.2002) AU

(71) Applicant *(for all designated States except US)*: **TYNEVALE PTY LIMITED** [AU/AU]; PO Box 673, 19 Church Street, Maitland, New South Wales 2320 (AU).

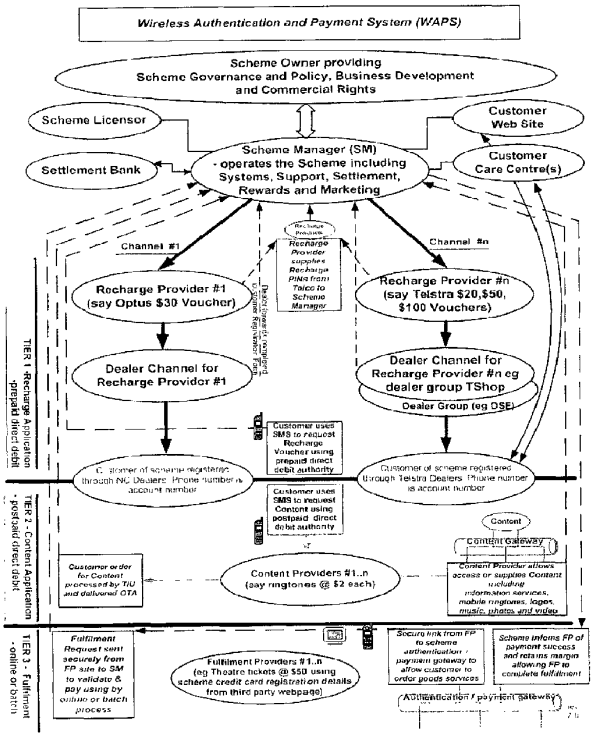
(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **REEVES, Peter, John** [AU/AU]; 21 Pollock Avenue, Wyong, New South Wales 2259 (AU). **SIMARD 3RD, Joseph, Arthur** [AU/AU]; "Lonou Park", 1524 Gresford Road, Torryburn, via Paterson, New South Wales 2421 (AU). **WANN, David, Paul** [AU/AU]; 7 Goonak Parade, Narara, New South Wales 2250 (AU). **PACKETT, Jayson, Geoffrey** [AU/AU]; Unit 2, 159 Denton Park Drive, Aberglasslyn, New South Wales 2320 (AU). **MORGAN-JONES, Mark** [AU/AU]; 95 Ridge Road, Kilaben Bay, New South Wales 2283 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR A WIRELESS PURCHASE REQUEST AND PAYMENT FOR GOODS OR SERVICES



(57) Abstract: Disclosed is a system and method that enables any subscriber to a wireless communications network to obtain wirelessly and instantly prepaid products and/or services by using their wireless device and by registering with a plan as a customer, and, allowing the plan to maintain the prepayment of the prepaid products and/or services from the customer's financial institution account or facility. Further, customers are able to purchase products and/or services on a non-recurring entitlement basis instantly and to pay for the products and/or services by a subsequent funds transfer to the plan. Furthermore, customers are able to purchase products and/or services from approved third parties through the third parties website, mail order service, phone order service, wireless service or other methods using a secure link to the plan's authentication and/or payment approvals methods.

WO 2004/023353 A1

SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designation US*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR A WIRELESS PURCHASE REQUEST AND PAYMENT FOR GOODS OR SERVICES

Technical Field

The present invention relates to a new type of system for and method of the purchase of goods or services using the transmission of a purchase request via wireless means, and in particular to the purchase of goods or services whereby the purchase is requested by a mobile handset user via the mobile handset. Also in particular, the present invention relates to a computer program which facilitates a wireless request for the purchase, access or rental of goods or services by a mobile handset user making use of the mobile handset.

More particularly, the present invention relates to the wireless transmission by a mobile handset user of a purchase request for a prepaid mobile handset voucher, and a means for effecting payment for the prepaid voucher.

Background Art

Presently, it is known to provide a user of a mobile handset with access to a communications network by allowing the user to purchase prepaid mobile handset vouchers, the value of which can be applied to the user's prepaid mobile handset account, from organisations offering such prepaid vouchers. For example, in Australia a user can purchase preset values of prepaid vouchers (i.e. mobile handset recharge cards) from a telecommunications service provider, such as Telstra (an Australian company), or an authorised reseller. This allows the user to access a telecommunications network and associated services with a mobile handset, and also sets limits on the costs incurred by the user (i.e. the value of the prepaid voucher) for use of the telecommunications network or associated services.

To make use of this service a user is required to establish a "prepaid account" with a telecommunications service provider (i.e. telecommunications carrier), through an authorised retail outlet. A prepaid voucher can then be purchased by the user from a retailer. To use the prepaid voucher the user dials a number supplied by the telecommunications service provider and types in via the mobile handset keypad, the designated prepaid voucher number which appears, usually as a string of numeric and/or alpha digits, on the prepaid voucher. This acts to apply credit to the user's prepaid account which has previously been established with the telecommunications service provider.

Prepaid vouchers (i.e. mobile handset recharge cards or the like) can presently only be bought from certain retailers. A user, or someone else on behalf of the user, is required to attend the premises of such a retailer and purchase a prepaid voucher. This situation has disadvantages. For example, the user is required to physically attend the premises of the retailer. Furthermore, the user cannot access a telecommunication network if the credit in the user's prepaid account has been exhausted other than to access the toll free IVR system for recharging and the user cannot purchase a prepaid voucher, which may occur, for example, if retailers are closed.

This identifies a need to provide a user with a prepaid voucher via wireless means, for example by transmitting the prepaid voucher to the user's mobile handset. A further problem then also arises, concerning how to retrieve payment from the user for a wirelessly transmitted prepaid voucher. It would be possible to require the user to supply credit card details prior to sending a prepaid voucher to the user, and perform a funds transaction before delivering a prepaid voucher to the user. However, a problem with this approach is that generally most prepaid voucher users do not have credit cards. Furthermore, if direct debit accounts were to be used, funds cannot be deducted in real-time (due to technology and policy/regulatory restrictions). Organisations are reluctant to deliver goods or services to a user (i.e. customer) and then attempt to obtain funds afterwards through an overnight funds settlement process. This further identifies a need to provide a user with a prepaid voucher via wireless means and obtain payment for the prepaid voucher.

Also, at present, a user is limited in the types of payment systems with which the user can purchase various goods or services using a mobile handset. For example, it is known that at present a mobile handset user can purchase a mobile handset ring tone using a mobile handset by purchasing vouchers which entitle the customer to a number of ring tones. These tones are delivered to the mobile handset by dialling a number and entering in the code for the desired ring tone, or selecting the ring tone from a web site and entering the designated voucher number. This system has the same drawbacks of the current prepaid voucher system. Also, it is known that at present a mobile handset user can purchase cans of soft drink at specific locations by dialling a specified number on the delivery device (a vending machine). The funds are deducted from the user's account. {This system is at present limited to Telstra customers with a non-prepaid account and is currently not available for pre-paid accounts with any carrier.} Moreover, a user is limited in the types of goods or services which are able to be purchased or requested via a mobile handset. If the user does not have a credit card or an existing billing arrangement with an organisation, then the user is typically prevented from purchasing goods or services if the organisation requires payment before delivery of the goods or services to the user. Still furthermore, many users are reluctant to provide credit card details over the Internet or to an unknown organisation. This identifies a need for a new type of system for and/or method of the purchase of goods or services by using the transmission of a purchase request via wireless means, and associated payment means. This also identifies a need for a new type of computer program for facilitating the aforementioned systems or methods.

Definitions

As used herein the term mobile handset should be considered as equivalent to the term mobile phone, cellular phone, cell phone, car phone, satellite phone, module and the like. This includes all forms of mobile, transportable or portable telephones or handsets. The term mobile handset should also be taken to include any device which is able to connect to a wireless communications network and wirelessly transmit data, multimedia content or information to a remote device, for example a remote computer system, over the communications network. This could include, for example, mobile data terminals, personal digital assistants (PDAs), or pagers. The communications network infrastructure may include switches, base stations, bridges,

routers, or any other such specialised components, which facilitate the connection between a mobile handset and a communications network.

Prepaid account: is a mobile handset user's service subscription with a telecommunications or other industry sector service provider (or telecommunications carrier) which can hold an amount of credit (prepaid) which allows a mobile handset to access and utilise a service provider's network and associated services.

Prepaid voucher (or recharge card, recharge voucher, prepaid card, or the like): is purchased by the user from a service provider, reseller, retailer, or the like, and when activated or used applies credit to the user's prepaid account which has previously been established with the telecommunications or other industry sector service provider.

User account (or customer account): is the account held on a management computer system which holds information on the user's entitlement to be issued with a pre-purchased prepaid voucher.

Financial institution account (or bank account): is a monetary account or facility held by the user's financial institution or card issuer. The financial institution account can be debited after obtaining user authority.

Disclosure of Invention

In its various embodiments the present invention seeks to provide a system, method or computer readable medium of instructions which overcomes, or at least ameliorates, the aforementioned and other problems inherit in the prior art.

In a broad form, the present invention addresses existing problems by allowing a user to register with a payment system which pre-purchases a prepaid voucher. Preferably, the pre-purchase is via an overnight settlement process. After the transfer of funds is completed the user is registered with the payment system and a user account is appropriately credited. This could be thought of as pre-allocating a prepaid voucher to the user account, or an entitlement to a prepaid voucher, which the user can request when required. Hence, the user account holds an entitlement to a prepaid voucher which the user has already purchased and may request at any time. The process of requesting the prepaid voucher also triggers a process of deducting further funds from the user's financial institution account, which results in a new prepaid voucher being allocated to the user account for when next required by the user.

Preferably, the prepaid voucher is delivered to the user's mobile handset via the Short Messaging Service (SMS). In another form of the invention, the prepaid voucher could be delivered to the user via Enhanced Messaging Service (EMS) or Multimedia Messaging Service (MMS). The prepaid voucher could be delivered to the user by any other means over a communications or telecommunications network. It should be appreciated that any form of 'messaging' involving transmissions over a wireless network could be utilised to transmit the prepaid voucher.

When received the user then applies this prepaid voucher to the user's prepaid account with a telecommunications service provider. In another embodiment, the prepaid voucher can be directly applied to the user's prepaid account with the telecommunications service provider without the user being required to receive and then apply the prepaid voucher.

In another broad form, the present invention provides a payment system which allows a user to request, via a mobile handset, the purchase of goods or services which are paid for by management software debiting the user's financial institution account according to a pre-existing debit authority.

In a further broad form, the present invention provides a system which allocates an entitlement to a prepaid voucher to a user of a mobile handset, the entitlement to the prepaid voucher being recorded in a user account in a management computer system, and whereby the user can request the prepaid voucher be delivered via a mobile handset. Preferably, after the prepaid voucher is delivered the user's financial institution account is debited and an entitlement to a new prepaid voucher is recorded in the management computer system.

In still a further broad form, the present invention provides a system for allowing a user of a mobile handset, with the user having a prepaid account with a telecommunications service provider, to add credit to the prepaid account, the system including:

- the mobile handset operated by the user;
- a management computer system which is able to communicate with the mobile handset;
- management software resident in the management computer system, the management software including a user account, the user account recording any entitlement of the user to a prepaid voucher;
- a financial institution computer system which is accessible via some electronic means, whether in real-time or by a message sent to the institution, by the management computer system, the financial institution computer system holding a financial institution account for the user; and

whereby, in response to a request by the user, the request being wirelessly transmitted from the mobile handset to the management computer system, for a prepaid voucher, the management software transmits the prepaid voucher to the mobile handset and subsequently requests a transfer of funds from the user's financial institution account to a nominated bank account, which when confirmed, results in an entitlement to a new prepaid voucher being recorded in the user account.

In accordance with yet another broad form, the present invention provides a payment system for allowing a user of a mobile handset, the user having executed a debit authority enabling funds to be transferred from a financial institution account to a nominated bank account, to purchase goods or services from a third party using the mobile handset, the system including:

- the mobile handset operated by the user;
- a management computer system;

- management software resident in the management computer system;
- a financial institution computer system which is able to communicate with the management computer system, the financial institution computer system holding the financial institution account for the user;
- a third party computer system which is able to communicate with the mobile handset, the third party computer system used by the third party to receive requests for goods or services; and

whereby, in response to a request by the user for the purchase of selected goods or services, the request being wirelessly transmitted from the mobile handset to the third party computer system, the third party requests funds from the management computer system which results in a request for a transfer of funds from the financial institution account to a nominated bank account, which when confirmed, results in the management software transferring the required funds and a purchase request to the third party for the goods or services.

In another embodiment of the present invention, there is provided a method of providing a user with a prepaid voucher which can be used to credit a prepaid account with a telecommunications service provider, the method allowing the user to request and receive the prepaid voucher via a mobile handset, the method including the steps of:

- the user being registered in a management computer system;
- the user wirelessly transmitting a request for a prepaid voucher to the management computer system which hosts management software;
- the management software checking the status of a user account for user entitlement to the prepaid voucher;
- the prepaid voucher being transmitted to the mobile handset; and
- the management software causing funds to be transferred from a financial institution account in a financial institution computer system to a nominated bank account, which when confirmed, results in an entitlement to a new prepaid voucher to be recorded in the user account.

In yet another embodiment of the present invention, there is provided a computer readable medium of instructions residing on a management computer system, the computer readable medium of instructions forming part of a system for facilitating a user of a mobile handset to add credit to a prepaid account with a telecommunications service provider, the computer readable medium of instructions including procedures for:

- receiving a request for a prepaid voucher, the request having been wirelessly transmitted from the mobile handset to the management computer system;
- checking the status of a user account for user entitlement to the prepaid voucher;
- transmitting the prepaid voucher to the mobile handset;
- requesting a transfer of funds from a financial institution account to a nominated bank account; and when the funds transfer is confirmed,
- adding an entitlement to a new prepaid voucher to the user account.

In still yet another embodiment of the present invention, there is provided a computer readable medium of instructions residing on an management computer system, the computer readable medium of instructions forming part of a system which facilitates a user of a mobile handset to purchase goods or services from a third party using the mobile handset, the computer readable medium of instructions including means for:

- receiving a funds transfer request from the third party computer system;
- requesting a transfer of funds from the user's financial institution account in a financial institution computer system to a nominated bank account;
- sending a purchase request to the third party
- confirming the transfer of funds; and
- sending the funds to the third party for the goods or services.

According to one aspect the request by the user is an SMS request. In a broad sense the goods or services may be "content" which can be wirelessly delivered to the user's mobile handset. In a particular embodiment, the content is delivered directly to the user's mobile handset from a third party, or to the user's mobile handset via the management computer system. In a particular form of the present invention, the content is prepaid Internet recharge vouchers, mobile handset ring tones, logos, graphics, video, music, subscription services, or the like. In a further form of the invention the goods or services requested by the user may be delivered by physically delivering or picking-up the goods or services.

In one embodiment, the prepaid voucher is an SMS message as representative of a wirless message. In a particular form of the invention the management computer system sends a SMS confirmation of the user's request or purchase confirmation to the user's mobile handset or other nominated mobile handset. In accordance with another specific embodiment of the present invention the mobile handset is not the user's mobile handset. In a further embodiment of the present invention, the nominated bank account is nominated by a Manager of the management computer system. In a further particular embodiment of the present invention, the third party computer system is integrated with the management computer system. In still a further embodiment of the present invention, the nominated bank account and the user's financial institution account are not in the same banking computer system.

The present invention according to yet another aspect provides that the funds transfer is by direct debit from the user's financial institution account. In other forms, the funds transfer can occur using any other form of electronic payment, for example, credit card. In a further broad form of the present invention, the management software provides for the registration of user's, account processing and payment, and receiving user requests.

According to one embodiment of the present invention, the distribution channels (eg. dealers) receive an on-going revenue stream from pre-paid 'connections', similar to post-paid mobile connections.

In a particular form of the present invention the management software is based on the JAVA programming

language. In a particular form of the present invention, a Personal Identification Number (PIN) or password is required to be supplied by the user via the mobile handset before the user's request is processed.

In a further embodiment of the invention, the authentication is provided by an image of the users face captured by a camera contained or connected to the mobile handset and delivered to the biometric authentication component of the system. The face recognition process involves software within the system to generate a small file of approximately 2000 bytes known as a biometric template that represents the salient features of the user's face that can be understood by software in an authentication process to validate an image captured on the user's mobile handset and compared to/with or against the biometric template generated by the system. The face recognition process is triggered which verifies (within high bounds of statistical probability) that the user of the mobile handset is the same person enrolled in the system by comparing the user's biometric template created during the enrolment process and compared with the processed image either generated on the mobile handset or transmitted to a biometric authentication system allowing the system to authenticate the user. Further, content purchased or delivered by the system can be digitally signed (and encrypted if required) with the user's biometric template incorporated into the content to enhance the content owners rights to control and or monitor how the content is distributed including options such as authentication processes involving the user having to present their captured image to the system whenever the content is required to be accessed or played. In addition to purchasing and accessing content used in the system, this 'use of content transaction' could be used as a service to ensure secure delivery of emails and documents over the Internet requiring the user to authenticate themselves with the system's biometric authentication server whenever highly confidential emails, content or documents are required to be accessed either directly on the user's mobile handset or delivered to an Internet service or the user's email service. This embodiment of the invention provides a low cost method of biometric authentication without the user having to purchase personal authentication devices such as tokens or smartcards that must be carried by the user and readers (such as personal smartcard readers) to enquire and /or authenticate the physical token. The enrolment process which could be performed at the retail outlet would incorporate additional steps whereby the retailer would complete a new enrolment or update an existing users biographical enrolment data by confirming the enrolment systems pairing of the biographical enrolment data with the user's biometric template created when the user is directed by the retailer to connect to the system's biometric authentication system. The pairing occurs when the biometric authentication system captures a suitably framed image of the user's face using the user's camera on the mobile handset and creating the user's biometric template, displaying the user's image captured within the retailers online enrolment screen and requesting the retailer validate that the image displayed on their enrolment screen is of the person being enrolled by them. When the retailer confirms this to be the case, the system pairs the biographical enrolment data (including the user's financial institution account details and associated payment authority agreed during the enrolment process) with the user's biometric template created during enrolment. The user's biometric template can be stored on the system's biometric authentication server requiring to be paired with the user's biographical enrolment data whenever a financial transaction or use of content transaction is required to be performed. Alternatively, and subject to the technology embodied within the user's mobile handset, the

user's biometric template could be securely stored on either the smartcard that serves as the user's subscription identity module or in a secure 'electronic wallet' or similar concept incorporated into the user's handset. Alternatively, the further embodiment of the invention could provide for a biometric validation engine to be licensed by mobile handset manufacturers and incorporated into future mobile handset models that allow for the local authentication of the user's biometric template without having to connect to the system's biometric authentication system to provide authentication services. In this embodiment, the face recognition process would occur on embedded software within the handset and the software would send an authorisation token, rather than the captured image of the user, to the system during the purchase request.

Brief Description of Figures

The present invention should become apparent from the following description, which is given by way of example only, of a preferred but non-limiting embodiment thereof, described in connection with the accompanying figures, wherein:

Figure 1 illustrates a broad schematic of an embodiment of the payment system;

Figure 2 illustrates a broad schematic of a specific embodiment of the method of the present invention;

Figure 3 illustrates the main use cases according to an embodiment of the present invention; and

Figure 4 illustrates a logical view of the main entities of a particular embodiment of the present invention.

Modes for Carrying Out the Invention

I Overview

Referring to figure 1, a general schematic of the payment system 10 is illustrated. The user 15 has access to a mobile handset 20. The user 15 also has a user account 25 which is recorded in the management computer system 30. The management computer system 30 is administered or managed by a Manager (or Management organisation). The user 15 is additionally required to have a financial institution account 35 held in the financial institution computer system 40. Resident in the management computer system 30 is management software 45. The management software 45 can provide functions for processes such as user registration, account processing and payment, and receiving user wireless requests for a purchase, which could be for a prepaid voucher.

In use, the user 15 desires to purchase user selected goods or services from a third party or the Manager. The third party operates a third party computer system 50 which can at least receive requests for goods or services. Goods or services may include prepaid vouchers or prepaid starter kits for access to a telecommunications network and associated services, "content" such as mobile handset ring tones, logos, graphics, video, music, subscription services, etc, or any other goods or services which are required to be physically delivered to, or picked-up by, the user 15. Prepaid vouchers need not be physically delivered to the user 15, and "content" can be wirelessly delivered to the mobile handset 20, or any other nominated

mobile handset. A prepaid starter kit allows dealers to activate in-store a SIMcard with a new prepaid mobile service. Previously, the dealer received a package that contained the SIMcard and associated mobile handset number. This may be performed on-line from a retail store.

Prior to requesting goods or services, the user needs to be registered with the management computer system 30. This involves the user authorising the Manager to debit the user's financial institution account 35 when required. After registering, funds are transferred from the user's financial institution account 35 to a nominated bank account, the funds being used to purchase a prepaid voucher on behalf of the user. The user's entitlement to receive the prepaid voucher is recorded in the user account 25.

To request goods or services the user 15 operates the mobile handset 20 causing a wireless request 55a to be transmitted to the management computer system 30, or, an SMS request 55b to be transmitted to the third party computer system 50, depending on the goods or services requested. For example, if the purchase request is for a prepaid voucher, then the wireless request 55a is sent to the management computer system 30. If the purchase request is for "content" such as a mobile handset ring tone, then the wireless request 55b is sent directly to the third party computer system 50 offering the ring tone.

When the management computer system 30 receives the wireless request 55a, data or information in the wireless request 55a is passed to the management software 45. If the request is valid, the management software 45 causes a prepaid voucher in the wireless format 60 to be transmitted from the management computer system 30 to the mobile handset 20. If the wireless request 55a is for a prepaid voucher, then the management software 45 checks the user entitlement to a prepaid voucher by checking the user account 25. If the user is entitled to be delivered a prepaid voucher then the management software 45 effects the delivery of the prepaid voucher 60 as a wireless message to the mobile handset 20. The user 15 can then apply or activate the prepaid voucher by dialling a telehandset number indicated in the message. This applies credit, embodied as the prepaid voucher, to the user's prepaid account with the telecommunications service provider, thus enabling the user to access the telecommunications network and associated services.

Furthermore, once the prepaid voucher 60 has been delivered to the mobile handset 20 the management software 45 initiates a request for a further transfer of funds from the financial institution computer system 40, via the computer network 65. The management software 45 requests a transfer of funds from the user's financial institution account 35 in the financial institution computing system 40 to a nominated bank account. This request can be made immediately or at some later time. When the transfer of funds to the nominated bank account is confirmed by the financial institution computer system 40, an entitlement to a new prepaid voucher is recorded in the user account 25 within the management computer system 30. The user can then obtain this pre-purchased prepaid voucher when required in the future without waiting for funds to clear.

Hence, the user 15 is purchasing an entitlement to be sent a prepaid voucher (which may be referred to as a "prepaid prepaid voucher") for access to a telecommunications network and associated services offered by a

telecommunications network provider and the Manager is acting as a reseller.

When the user 15 requests "content", or other goods or services not being a prepaid voucher, an SMS request 55b is sent to the third party computer system 50. Depending on the nature of the goods or services, delivery, that is wirelessly or physically, and the third party itself, goods or services may be delivered prior to or after the transfer of funds associated with payment for the goods or services from the user's financial institution account 35.

Whether pre- or post- delivery payment is required, the third party computer system 50 can receive the user's purchase request. The third party bills the Manager according to its usual practice. When a request for a transfer of funds is received from the third party operating the third party computer system 50 the management software 45 causes the user's financial institution account 35 to be debited accordingly. The funds can then be transferred to the third party, for example to the third party computer system 50, and the Manager can retain a payment processing fee.

Alternatively, the SMS request 55a received by the management software 45 could be a request for content or physical delivery-type goods or services provided by the third party. The Manager could have an arrangement with the third party to offer selected goods or services. In this situation, the management software 45 can relay the user's purchase request to the third party computer system 50 via the computer network 70. Either before or after the goods or services have been delivered to the user 15 or the mobile handset 20, the user's financial institution account 35 can be debited and funds transferred to the third party (which could be confirmed by communication between the management computer system 30 and the third party computer system 50). It may be a condition in the arrangement between the Manager and the third party that funds must be transferred to the third party prior to delivery of goods or services.

II Modules

The following modules provide a more detailed outline of a particular embodiment of the present invention. The modules are intended to be merely illustrative and not limiting to the scope of the present invention.

System and Processes

This section contains various system and process definitions describing the various participants in the method or system and how the participants inter-relate with each other when conducting business within the method or system.

The method or system allows registered users (referred to as Customers in this section) of the method or system to purchase goods and services using a mobile handset. Registration involves a Customer providing an authority to the Manager to pay for goods or services ordered by the Customer.

Goods and Services

Goods and services that can be purchased by the Customer in the method or system can broadly be described as:

1) prepaid vouchers: (recharge vouchers) supplied 'over the air' to the Customer's mobile handset. Examples may include Optus' currently existing $30 mobile handset recharge cards, Telstra's currently existing $25, $60 and $100 mobile handset recharge cards;
2) content: that can be ordered and delivered 'over the air' to the Customer's mobile handset. Examples are mobile handset ring tones, logos, video, music, subscription services and other content;
3) fulfilment: of other goods or services ordered by the Customer through endorsed fulfilment methods using sales points provided by other parties such as websites, Wireless Application Protocol (WAP) sites, IVR and other emerging eCommerce technologies. Fulfilment goods and services are not delivered 'over the air'. Delivery is through traditional fulfilment methods such as by courier, mail, email or by Customer pickup. Examples are venue reservations, ordering goods from infomercials or anything that can be sold over the Internet.

Applications

Each of these three types of goods or services are generally distinct within the method or system and involve distinct 'Applications'. Applications are distinct business models, methods or systems involving different payment and delivery processes. The Applications supported by the method or system can include:

1) recharge vouchers: may be purchased using a prepaid direct debit method. This could also referred to as 'prepaid prepaid';
2) content: may be purchased using post-paid direct debit referring to the concept that the payment request is made after the goods or services are delivered; and
3) fulfilment: may be purchased using online authorisation of credit card authority.

In one embodiment of the invention, a Wireless Authentication Payment System (WAPS) is provided which caters for each of the Applications identified above.

System/Method Participants

Referring to figure 2, in a particular, but non-limiting, form of the present invention, the participants within the method or system can include:

(1) The Customer: is a prepaid mobile handset user who registers with the management computer system by providing financial institution account details authorising the Manager to purchase goods or services ordered by the Customer. The Customer might be required to pay the full retail price of a recharge voucher as if the Customer purchased the recharge voucher from a store.

(2) The Dealer Channel(s): functions to register the Customer to the method or system. The Dealer Channel comprises Dealer Groups identified and branded with the recharge products available through the Dealer Channel. Each Dealer Group includes:

- a Dealer Franchiser; and
- Dealer Franchisee(s) operating under the governance of the Dealer Franchiser.

When Customers are registered through the Dealer Channel, the Dealer Franchiser and the Dealer Franchisee registering the Customer receive a percentage of every recharge voucher purchased by the Customer as an ongoing commission;

(3) The Recharge Provider: performs two functions within the method or system:

- introduces one or more Dealer Groups to form the Dealer Channel to participate in the method or system; and
- provides (acquires and sells) recharge vouchers to the Manager as a supplier for the recharge products ordered by Customers signing up through the Dealer Channel.

The Recharge Provider bills the Manager for the supply of recharge vouchers making a margin on their cost price. The Recharge Provider does not receive a commission from the Manager.

(4) The Booking Provider: provides content for the method or system that can be ordered and delivered 'over the air' to the Customer's mobile handset. The Booking Provider establishes a retail price for their products; the Manager retains a margin of the transaction value.

(5) The Fulfilment Provider: provides goods or services that are not delivered 'over the air' to the Customer's mobile handset. Instead of paying by VISA, AMEX or Mastercard, etc., a Customer chooses to pay using the prepaid mobile handset account held in the system. The Fulfilment Provider should be authorised by the System Owner to cobrand their sales point (eg. website, WAPsite, IVR, infomercial, etc). The Fulfilment Provider establishes a retail price and the Manager retains a commission from the Fulfilment Provider when processing the Customer payment for goods or services ordered using the system or method.

(6) The Manager: provides the operations management functions of the system or method including hosting the system and registration databases, providing dealer support, settlement and reporting services to the various participants, marketing and assumes responsibility for any reward programmes that may be established. In addition, the Manager can also provide oversight and/or outsources a Customer Care Centre and a Customer website service provision. The Manager may make a profit on the difference between the retail price charged to the Customer less the commissions paid to the Dealer Channel, to system support, to clearing payments through the bank, payment of merchant fees, bad debts and the cost to maintain the Customer Care Centre and the Customer website.

(7) The System Licensor: is regarded as the provider of the management software to the system. The System Licensor may provide an exclusive licence to the System Owner and/or Manager to use the management software The System Licensor may be paid a transaction fee as a percentage of each Customer

purchase made in the system. The System Licensor may also be responsible for the maintenance and upgrading of the management software.

(8) The System Owner: is regarded as the owner of the system. The System Owner provides the System Governance and Policy, Business Development and determines Commercial Rights. The System Owner may provide an exclusive or non-exclusive licence to the Manager to use the system.

System Definition and Processes – The Customer

The system or method enables prepaid mobile handset Customers the ability to buy vouchers (prepaid recharge cards) using a mobile handset 'over-the-air' anywhere and at any time effectively using a bank account. This allows the Customer the 'best of both worlds', that is all the convenience of a post-paid account handset with all the advantages of a prepaid account including lower call costs, superior cost control and no minimum spending requirement.

The system requires the customer to register with the system using a password so that the account is secure. Registering with the system can be performed at an authorised dealer or can be performed using a website.

Part of the registration process involves signing a Direct Debit Authority authorising the Manager to purchase vouchers using the Customer's bank account. Whenever a voucher is ordered by using the mobile handset to send an SMS request, the voucher is sent almost immediately by being previously purchased using the bank account. This also allows a parent to control the use of a prepaid account that can be set up for use by a child or teenager. The parent is identified as the Account Holder and the child/teenager as the Account User, with the parent safe in the knowledge that the account can be used when required, and that the parent knows when vouchers are bought, and also that the prepaid account is secured by a password that only the parent (as the Account Holder) knows.

Furthermore, the system or method can include many advanced features such as 'Any Mobile' which allows credit to be bought, even if a Customer does not have any credit left in the prepaid account, by using another mobile handset, for example a friend's mobile handset.

A Customer can also:

purchase low value content that can be delivered 'over the air' to a mobile handset or like device. Current examples of such content are mobile handset ring tones, logos, video, music, information services and other content. A bank account or similar can be direct debited to the value of content ordered from the mobile handset or through an authorised website;order or book higher value goods or services over authorised Handset, websites or WAPsites using credit card registration details as the payment method. Using the system as a payment method provides confidence because a Customer does not need to supply credit card details over the handset or over the Internet.

System Definition and Processes – The Recharge Application

The Recharge Application is the business architecture of the system which allows Customers to register with the system through authorised storefront dealers or approved association organisations. Customers are required to 'register' with the system. Registration occurs when a customer signs up at an Authorised Dealer or other location.

A Dealer Channel includes one or more Dealer Groups associated with a Recharge Provider. A Dealer Group includes a Dealer Franchiser and Dealer Franchisees operating under the governance of the Dealer Franchiser. The system allows for multiple Dealer Groups associated with the introducing Recharge Provider and allows for multiple Recharge Providers within the system architecture. Collectively, this arrangement forms the participants of the Recharge Application, specifically, the collection of Recharge Providers each having contributed Dealer Channels, each of which is represented by Dealer Groups, each of which is identified as the Dealer Group Franchiser and the collection of Dealer Group Franchisees.

A Dealer Channel is typically identified as the collection of Dealers selling one or more brands of recharge card or voucher. As a non-limiting example, at present the Australian market would allow the system to have the following Dealer Channels marketing the following prepaid recharge voucher values:

Optus - $30 mobile vouchers, Optus - $14.95/7hr, $19.95/15hr, $34.95/30hr and $44.95/60hr internet vouchers; Telstra - $25, $60 and $100 vouchers; Virgin - $15; Vodafone - $20, $30, $50, $100 mobile vouchers; AAPT etc.

The system is flexible and allows for any combination of the following types of Recharge Application models which are provided as illustrative examples.

Example 1 – Dealer Group becomes the Recharge Provider.

A Dealer Group (say Network Communications – an Optus Premium Dealer) may negotiate the role of the Recharge Provider and introduce its dealerships to form a Dealer Channel. Network Communications dealerships could all be branded with Optus and the Manager brand.

Example 2 – Telco Introduces balance of Dealers

As an extension of example 1, Optus Communications may negotiate the role of the Recharge Provider and introduce the balance of its Dealer Groups (say Optus World, C21, Tandy and Strathfield Car Radios) to form a Dealer Channel. In this instance, there would be two Dealer Channels providing Optus recharge vouchers. The balance of Optus Dealer Groups would all be branded with Optus and the same Manager brands for both Dealer Channels. The Customer would not be able to discern that there are two Dealer Channels.

Example 3 – Telco introduces all its Dealers.

A telecommunications company (say Telstra) may negotiate the role of the Recharge Provider for the Telstra Dealer Channel with Franchisors for Tshops, DSE, Strathfield Car Radio, etc., introducing their Dealer Franchisees within their respective Dealer Groups to form the Dealer Channel.

Further, Telstra may decide to brand the system as its own product. Subsequent to negotiations with the System Owner, Telstra are licensed as a Manager of their own system and brand the system distinctly from the system described in Example 2.

Example 4 – Dealer Group participates in two different Dealer Channels

If examples 2 and 3 were to occur at the same time, the Dealer Group Strathfield Car Radio which holds dealerships with Telstra and Optus, could participate in two different Dealer Channels of the system at the same time. Customers registering through this Dealer Group would register with the Dealer Channel associated with the Customer's recharge voucher.

Dealer Groups receive ongoing commissions subject to commercial rights negotiated with the respective Recharge Provider and the currency of their dealership arrangement with the Dealer Channel to which their Customers are signed. In example 2, if Tandy were to lose their status as dealers in the Optus Dealer Channel, the Tandy Dealer Group would not receive any additional commission payments subsequent to the date of disassociation for Customers registered through that Dealer Channel. If Tandy participated in another Dealer Channel, Tandy would not be required to remove branding with the system and would continue to receive commissions generated through the other Dealer Channel.

When Customers are registered through the Dealer Group, the Dealer Franchiser and the Dealer Franchisee registering the Customer may receive a percentage of every recharge voucher purchased by the Customer as an ongoing commission with the Recharge Provider supplying Recharge Vouchers as appropriate. Unless commercial arrangements are made between the System Owner and the Recharge Provider, participants in the Content Application generally do not receive commissions from Customer purchases made within either the Content Application or the Fulfilment Application.

The system automatically generates settlements and settlement reports for commissions earnt by the members of the Dealer Groups within the Dealer Channel. Settlement may occur overnight, weekly or monthly subject to the terms of settlement negotiated by the Manager with the Recharge Provider on behalf of the Dealer Group. The Manager can provide support to the Dealer Group.

System Definition and Processes – The Content Application

The Content Application is the business architecture of the system that allows registered Customers within the system to purchase Content to be delivered to their mobile handset using either existing or future 'over the

air' or wireless technologies. Examples of Content that can be purchased are mobile handset ring tones, logos, screen savers, video, music, subscription and information services and other content.

There may be multiple Content Providers to the system. Content Providers can be authorised by the System Owner to participate in the system. Content Providers can provide access to the Manager for the Content through a Content Provider's 'Content System'. This may be through a technical interface to the Manager or directly supplied by the Content Provider and managed by the system. Collectively, this arrangement forms the participants and mechanisms of the Content Application, specifically, the collection of Collection Providers, and Content Systems and interfaces.

Each Content Provider provides a number branded to the Content Provider and distinct to the Request Number for the Customer to send SMS requests to order Content. The Content Provider is responsible for their own point of sale material, branding, content and content selection menus / content item numbers. When a Customer orders Content, the Customer send an SMS request to the Content Provider's Request Number, thus ordering an item. The message format could be agreed with the Manager to ensure consistency throughout all Content Providers.

If the order is accepted, (i.e. the Customer's account status is 'active'), then the ordered Content is delivered over the air to the Customer's mobile handset. This may be via SMS or another wireless delivery mechanism. The Customer's debit authority is used to draw funds to the value of the content ordered independent of any recharge process.

System Definition and Processes – The Fulfilment Application

The Fulfilment Application is the business architecture of the system that allows registered Customers within the system who have registered credit card details to purchase goods or services from Fulfilment Providers.

Fulfilment Providers sell goods or services through sales points that in addition to providing payment methods such as VISA, AMEX or Mastercard are authorised by the System Owner to offer payment using the system as a payment method. The sales point may be a website, WAPsite, IVR or infomercial, which is cobranded with the System Owner brand or other indicative indicia.

The Fulfilment Provider establishes a secure connection to the system to transmit online payment requests and to accept or decline the payment request. The Fulfilment Provider establishes a retail price and the Manager retains a commission from the Fulfilment Provider when processing the Customer payment for goods or services ordered using the system.

System Definition and Processes – System Management

The system uses software and operating processes designed and developed according to industry and security best practice guidelines and compliant with relevant legislation. The system is managed by the Manager. The

Manager implements aspects of system management including system processes and support including the backend systems, databases, technical architecture, interfaces to a settlement bank, Call Centre and websites.

The following concepts are backend processes or procedures that enable the system to functionally operate.

Processing States

The system handles the processing of Accounts using logical states known as Processing States. The Processing States include:

- PreRegistered, PreRegistered_BadDebt and PreRegistered_BadBank which describe Accounts before they can be used by the customer:
  - *'PreRegistered'* means the Account has been created and the initial payment request has been made but not cleared;
  - *'PreRegistered_BadDebt'* means the Account has been created and the initial payment has been declined by the Customer's bank. No further processing occurs until the Customer advises sufficient funds are available. When notified, the state is reset to PreRegistered which restarts the payment request process;
  - *'PreRegistered_BadBank'* means that the Account has been created and the initial payment request has been rejected as the Customer Bank Account Details are incorrect. No further processing occurs until the Customer supplies their correct Bank Account Details. When corrected, the state is reset to Pending which restarts the payment request process;

- Active, Pending , Bad Debt and Bad Bank are normal processing states once customers start using the system:
  - *'Active'* means the Account has an entitlement to a Voucher which can be immediately sent to a Customer who Requests a Voucher;
  - *'Pending'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a voucher and that the system has not received notification that funds have cleared;
  - *'Bad Debt'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a voucher which has been declined by the Customer's bank. No further processing will occur until the Customer advises sufficient funds are available. When notified, the state is reset to Pending which restarts the payment request process;
  - *'Bad Bank'* means that the Account does not have an entitlement to a Voucher, the system has requested a payment on the Customer's bank to initially allocate or replace a Voucher and has been rejected by the Customer's bank as the bank account details are not recognised. No further processing occurs until the Customer supplies correct Bank Account Details. When corrected, the state is reset to Pending which restarts the payment request process;

- *'Cancelled'* is a state when the Account has been closed and the Customer can no longer use the system without Re-Registering.

Staff Roles

The system is administered and operated by the following staff categories performing roles that provide appropriate security access and controls to perform their operational responsibilities.:-

- Scheme Operators (SOs) – perform all the back office registration functions for the system including:
  - data entry of new applications and re-registering Customers;
  - the completeness and accuracy of information received and entered is correct;
  - the scanning and filing of registration information;
  - the initial 'Draw Down' of funds is completed correctly;
  - Bad Debts and Bad Bank processing of PreRegistered accounts is handled correctly and ;
  - that Accounts are Activated correctly.
- Scheme Administrators (SAs) – have full access to all of the operational management functions of the System and perform
  - Customer complaint resolution;
  - operational fraud management of the system;
  - cancelling customer accounts that are not initiated by the Account Holder;
  - acquirer bank settlement functions including
    - preparing and uploading Bank Bulk Funds Movement Files;
    - downloading and preparing Bank Settlement Files;
    - Process Account Statements;
    - manual oversight of closing open settlement batches within 2 business day window as required.
- Financial Administrator (FA) - is responsible for the financial management of the system or method including the financial management of the company with specific system responsibilities for
  - replenishment of PINs to the Unallocated Voucher Pool from the voucher supplier;
  - for internal audits of the system including manual and automatic processing;
  - processing dealer invoices and making settlement to Dealers;
  - oversight of settlement functions.
- Customer Care Operator (CCOs) – performs all Call Centre functions for calls received by the system including cancelling of accounts at Account Holder request. Complaints are deferred to an Administrator. CCOs also provide information on how to register for the system including mailing or emailing application forms upon request.
- Dealer Manager – overall responsibility for dealer management including
  - dealer appointments;
  - dealer training;

- dealer support;
- generating and providing dealer reports;
- dealer complaints resolution; and
- dealer collateral.

- Technical Support (TS) – overall responsibility for IT Systems, support, archiving, compliance with privacy and security policies, disaster recovery and system security.
- Operations Manager – responsible for the overall operation of the system.

Activate an Account

'Activate an Account' is an automatic process that changes the processing state of a PreRegistered Account to an Active Account. This process will occur whenever the Initial Draw Down results in the funds being cleared by the Customer's bank account. The Customer is notified the Account is Activated when the system sends the Customer a 'Welcome Message' by SMS. The Account can now be used by the customer to 'Request a voucher' from the system.

Request a Voucher

'Request a voucher' refers to a process that occurs whenever a Customer sends their password via SMS to the system's SMS server which upon receipt will validate the identity of the SIM in the mobile handset sending the SMS, authenticate the identity of the SIM against the Customer registration database and verify that the password is valid.

Deliver a Voucher

'Deliver a voucher' refers to a process where the system has received a 'Request a voucher', has verified the Customer's password, confirms that the Customer's Account is Active and then sends and validates an SMS that is delivered to the Customer's mobile handset which contains a Voucher number that the Customer can subsequently use to credit their prepaid handset credit.

Bad Attempts

'Bad Attempts' occur when either a Customer does not send a valid 'Request a voucher' or an attempt is made to defraud the system.

Account is Blocked

The system does not ignore 'Bad Attempts' and writes attempts to a 'Potential Fraud Log File'. When threshold levels are reached, the system restricts the operation of an Account by flagging the Account as Blocked. Blocking an Account will allow normal processing of States to occur, such as 'Draw Downs' and clearing of payments, however when an account is Blocked, the system will not allow a Voucher to be delivered nor respond by continuing to send error messages via SMS to the requesting mobile handset.

Draw Down

'Draw Down' refers to a process where the system attempts to receive a payment from a Customer's bank account prior to the system providing either the initial Voucher (Initial Draw Down) or to purchase a replacement Voucher to replace a Voucher after a recent 'Voucher Delivery' to the Customer using SMS.

Batching of Customer Payment Requests – Bulk Funds Movement File

The system uses an acquirer bank and software created by the bank to upload Customer payment requests in a Bulk Funds Movement File (BFMF). The BFMF is manually created by an Administrator using the system, generally before a 5 pm settlement deadline each business day. When the BFMF option is run, the system processes all Customer payment requests to the acquiring bank in batches of nominally 100 transactions. The system creates a batch identifier that is associated with transactions within the batch to allow for cross referencing. The transactions uploaded are settled overnight by the acquirer with each of the Customer bank accounts associated with the payment request transactions.

Bank Settlement file

'Bank Settlement File' refers to the file that is downloaded each morning using the acquirer bank's online banking facility. The Bank Settlement file shows all batches that were settled in whole or in part the previous evening. For each batch in the file the system can interpret:-

- the batch identifier for that batch;
- A= the batch total of the customer payments requested in that batch;
- B= the batch total cleared to date in that batch;
- C= details and value of individual rejected transactions in that batch and;
- D= details and value of individual rejections of a bad debt type in that batch.

Consequently E (the value of transactions that have not cleared, not rejected or not declined for payment) can be represented in the equation $E = A - (B + C + D)$

Process Account Statements

'Process Account Statements' refers to a clearing process which processes the content of all Bank Settlement files that have Open batches. If a batch is Open, the system knows that some Customer transaction in the batch have not been accounted for by the acquirer bank. Consequently, the batch is still open if $E > 0$. If all Voucher values are equal, then the value of E is a multiple of the Voucher value and the multiple represents the number of payment requests that are still to be settled by the acquirer bank.

If a batch is Closed, the system knows that every Customer transaction in the batch has been accounted for as either cleared (payment received), not cleared (a bad debt) or not processed (a bad bank) by the acquirer bank. Consequently, the batch can be closed when $E = 0$.

When the Process Account Statement option is run :

- transactions that have been declared as Bad Debts in the Bank Settlement File will result in the state of Customer's Account being changed to either PreRegistered_BadDebt or Bad Debt; and
- transactions that have been declared as Bad Bank in the Bank Settlement File will result in the state of Customer's Account being changed to either PreRegistered_BadBank or Bad Bank.

When the Process Account Statement option is run and results in the batch being Closed, transactions that have not been declared as Bad Debts or rejected as Bad Bank have been settled in full by the acquirer bank. Every one of these transactions can automatically cause the state of the Account associated with these transactions to be set as Active and the system can move a Voucher from the Unallocated Voucher Pool to the Allocated Voucher Pool and create an entitlement to the voucher to the Account.

Manually Closed Batch

'Manually Closed Batch' refers to a manual process that is performed to Close a batch that has not been closed automatically by the system within the prescribed two business day window allowed for a Draw Down to be completed. Adjustments in respect of the unaccounted transaction(s) are followed up with the relevant customer and bank as soon as practicable. This should be an irregular event. Batch size is configurable. By limiting batch size, the system can realise a higher closure rate on Day 1 processing.

Business Day 1 - Friday

Assume a batch of Customer Payment Request is created on Friday afternoon. Settlement is performed over night with a 4pm cutoff (business nights only). If the Batch is closed the morning following the first settlement (Saturday), all transactions that have cleared can be processed on Saturday or within one business day.

Business Day 2 - Monday

Assuming the batch is not closed on Saturday. The batch can be reprocessed over night on Monday, being the next business day. If the Batch is closed the next morning (Tuesday), all transactions have cleared on Tuesday or within two business days.

Under the Service Level agreements operating with Direct Debit Authorities, it is not expected that any batches should survive as Open beyond two business days.

It is recommended that if a batch is still Open after Business Day 2 that

- calls are made to the acquirer bank to determine why the batch has not closed
- and that by 4pm, that a 'Manually Closed Batch' option is performed

This means that all batches should be closed within two business days.

III Software Architecture

The following description describes a preferred, but non-limiting, embodiment of the software architecture which can be used to provide the system or method. Various other types of software architecture could equally be used and should be considered to be within the scope of the present invention.

Introduction

This section describes the software architecture for the Wireless Application Payment System. The system is a system to allow product purchase and/or delivery and/or confirmation using SMS or other wireless communication methods-initiated transactions.

The first application of the software is to allow delivery of a prepaid mobile handset voucher to a Customer via SMS, at the request of the Customer from an SMS message, and the Customer's account to be credited with another prepaid voucher after a successful transfer of funds from the Customer's bank account to the Scheme Manager's bank account. Other applications which can extend the system include delivery of ring tones and other products capable of being delivered to a Customer's mobile handset, and purchasing of products by registered users of the system using the funds transfer mechanisms of the system. The system does not preclude purchasing of a product via other means (such as through web-based interfaces), where the confirmation of purchase is performed using the wireless technology.

Overall Description

The system contains a service that accepts SMS messages and forwards the message to the J2EE processing and settlement engine via JMS. This service also receives messages from the JMS bus and sends the message via the SMS device/gateway. The J2EE processing and settlement engine receives messages from the JMS bus and processes these messages, which are normally requests for products. The engine is implemented as a collection of EJB session and message-driven beans.

The system also contains a Java, wing-based GUI for maintaining the application reference data, Customer registrations, system participants, and financial information. Referring to figure 3 and figure 4 the following use cases represent the architecturally significant use cases in the system.

Register Customer

- Customer details are entered into a screen from a paper registration form.
- The Customer details are checked against the current database for consistency: specifically, is this Customer already registered (duplicate mobile number), or is

someone else registered using this mobile number. Also, BSB and account number is checked against the database and a warning is flagged to the operator.

- Customer Password is preferably 4-6 alphanumeric characters but is configurable to any system requirements.
- If the Customer registration is successful, a NewVoucherRequest record is created to allow the initial voucher credit against the Customer's account. The Customer record is in a state of "Pre-processed" until the request is processed.

Process Account Statement File

- User selects the file
- File is opened
- For each record in the file:
  - Extract the account or batch reference
  - If it's a WAPS entry:
    - If the amount is –ve and there is a WAPS account reference,
      - Check for duplicates
      - create a bad debt
      - set Customers account to "BAD_DEBT"
      - find the outstanding NewVoucherRequest record and set its status to "FAILED"
    - If the amount is +ve and there is a batch reference
      - Check for duplicates
      - Find the DirectDebitBatch and set the "ActualAmount"
- Perfom the Settle Outstanding Accounts use case.

Settle Outstanding Accounts

- Find all DirectDebitBatch records which are not "CLEARED"
- For each batch:
  - If the Amount and ActualAmount are different, and the sum of the bad debts for this batch is not equal to the difference, do not clear the batch

- To clear the batch, execute the "Clear Funds for NewVoucherRequest" for each item in the batch for which there is no bad debt.

Clear Funds for New Voucher Request

When a debit was successful, the new voucher request was successful and the Customers voucher account is credited and funds from the payment are settled.

- Set status to cleared
- Apportion funds to participant accounts using the margins contained in the RechargePlan. Credit these amounts as new AccountLineItem records for each ParticipantAccount.
- Update the Customer's account by setting a voucher credit to the account and setting the state to "ACTIVE".

Process Prepaid Voucher File

- User selects File
- Create a voucher file record
- For each record in the file, add the record to the database

Process Recharge Request

Main Flow

- System receives an SMS
- The sender is validated against the account database
- The PIN in the message is validated against the database
- If the account status is in credit then send an SMS using the next voucher from the pool
- Update the account status (set to "PENDING") & creates NewVoucherRequest transaction (used by the Create Direct Debit use case) and sends the SMS

No credit:

- Check the time of the last successful NewVoucherRequest. If it is within the last hour,
- If there have been 3 or more resends in the last hour, ignore it, otherwise:
- resend the PIN and remember the resend.

- Otherwise , if there has been less than 3 errors in the last 24 hours, send a "No voucher credit" message

Invalid Password:

- For the first three occurrences, send a message "Invalid password (n/3)"

Alternatives

- The number of invalid password attempts or no credit attempts is configurable
- The messages sent in the SMS is configurable

Create Payment File

- User selects participant type and participant.
- If the participant type is Dealer, then the user selects a Dealer Group and the "Create Dealer Payment File" use case is executed for the whole group. Otherwise:
- Create a FundsTransferFile and a physical batch file with a line item that is a credit to the participant's bank account.
- The amount is the sum of all uncleared line items in ParticipantAccount for that participant.
- All line items are set to "cleared"

Create Dealer Payment File

- Create a FundsTransferFile and a physical batch file
- For each dealer:
  - Add up all the Amounts for the Dealers account that have not been cleared and add the total to a line item in the file. The line item will be a credit to the dealers bank account.
  - All line item amounts are set to "CLEARED".

Maintain Users

- Users have 1 or more roles corresponding to the actors in the specification
- Each function is associated with one or more roles
- The system will validate that the user has the appropriate rights to perform each use case by checking the role(s) of the user

Create Direct Debit File

- Create a new direct debit file (using date for filename)
- For each unprocessed CustomerAccountDebit transaction:
  - Add it to the DD file
  - Mark it as processed (link it to the debit file db record)

Supplementary Requirements

- The number of unsent vouchers, minus the number of outstanding requests, must appear on a main menu.

IV Appendix A

Attached in Appendix A is a narrative of example scenarios of the present invention in actual use. These scenarios are intended to provide an understanding of the various embodiments of the present invention and are not intended to limit the invention in any way. The scenarios are illustrative examples. Reference to "TopItUp" in Appendix A should be read as a reference to the system or the method, the Manager or the System Owner as appropriate.

Thus, there has been provided in accordance with the present invention a system or method, or a computer program, which satisfies the advantages set forth above.

The invention may also be said broadly to consist in the parts, elements and features referred to or indicated in the specification of the application, individually or collectively, in any or all combinations of two or more of said parts, elements or features, and where specific integers are mentioned herein which have known equivalents in the art to which the invention relates, such known equivalents are deemed to be incorporated herein as if individually set forth.

Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions, and alterations can be made herein by one of ordinary skill in the art without departing from the spirit or scope of the present invention.

APPENDIX A

Scenarios

Scenarios are a method of telling a narrative which provides insight and understanding into the workings of a system or scheme.

Instore Registration Scenarios

Customer Types

John Evans lives at Port Kembla and travels to work at Hornsby each day by train. His wife Kristy works in the local pharmacy three days per week and walks to work They are blessed with two sons Mark aged 15 and Matt aged 10. Mark and Matt both travel to school by bus. As a typical family with both parents working, being together as much as possible, keeping in touch and personal safety issues are key values in family decisions.

John has an office job and has a company supplied handset as he is often required to be contactable out of hours. John will occasionally ring Kristy on her mobile or the home handset when travelling home from work to arrange important family matters such as 'do you want me to bring anything home', 'what's on for dinner' or 'can you pick me up'.

Kristy bought a mobile handset three years ago on a $20 a month access fee plus calls plan with Telstra. The handset has worked great but is now considered bulky by modern standards. Until recently, she used the handset to be contactable, to make emergency calls at work and for personal safety reasons walking to work. Recently, Joanne, a friend in her Wednesday bridge club showed her how to use SMS and Kristy now regularly sends SMS to John to pick up groceries etc on his way home. Joanne has a Nokia 3310 prepaid mobile that she bought from Network Communications at Wollongong and has been encouraging Kristy to get a new prepaid handset from them since they really helped her when she was getting started.

When Matt gets home from primary school each day, Mum asks him to ring her on her mobile to let her know that he got home safely. Sometimes the school bus is not that reliable getting to school, particularly as the timetable has changed twice in the past three months. On two occasions recently, Matt has waited with other primary school kids at the bus stop for twenty minutes after the bus is due. He had been told that if ever missed the bus to go back home and ring Kristy at work.

Mark's 16th birthday is next Thursday. Half of the kids in Mark's class already have mobiles (mostly prepaid). Mark has had a keycard for four months. His allowance is paid into his account each month by Dad using internet banking. During the winter months, Mark stays back after school for soccer training. Mark gets home twenty minutes later than Matt. Mark doesn't have to ring Kristy unless his plans change at school. He has used a friend's mobile in the past.

Matt's bus incidents have caused great concern for his parents. They decide to get a new prepaid mobile for both Kristy and Mark. Mark's handset is to be his birthday present. Kristy is going to pass on her old handset to Matt.

On Saturday , they go to the Network store Joanne recommended to Kristy. After talking to Lee, the salesperson, they choose to port Kristy's number from Telstra to her new Nokia 3310 Optus prepaid handset using a port pack. Mark gets a new Optus prepaid Nokia 3310 and faceplate. Matt gets an Optus prepaid starter kit and a new faceplate for the Nokia 5110. Lee demonstrates the handsets and explains to the Evans's the various options for topping up their handsets. .

Customer InStore Registration

Lee knows that Prepaid is becoming a very significant proportion of his business while at the same time postpaid connections have dropped alarmingly. He's all too aware that despite the increased prepaid handset bundles and starter kit sales since prepaid was launched some four years ago, the number of customers topping up each month at his store is dramatically less than the number of prepaid connections he has done, even allowing for customers churning or cancelling their service. Lee knows these customers of his are topping up somewhere else and this loss of revenue coupled with the reduction in contract customers is adversely affecting his business. He's convinced that TopItUp is the way to increase his income by signing up prepaid customers to the TopItUp system simply because it ensures that he receives every TopUp his customer purchases no matter where and when the customer decides to TopUp. He also is pretty happy about the fact that he doesn't have to worry about receiving anymore prepaid TopUp invoices from Optus or, in relation to these invoices, not having enough money to pay his hardware account as TopItUp administer all that. Lee also knows that eventually TopItUp can, in the future, be used by him to sell other products and services thereby providing even more income for the store and the Network vision.

He therefore pulls out a TopItUp User Guide brochure and explains the advantages of topping up their handsets using TopItup over existing methods. Lee explains further that TopItUp gives them the 'Best of Both Worlds' being 'Prepaid Prepaid'. TopItUp allows them the convenience of an account handset in that they can TopUp over the air whenever and wherever they want to. At the same time, TopItUp provides all of the advantages of a prepaid account including lower call costs, superior cost control and no minimum spends.

After having spent some time with the Evans's, Lee knows that the primary reason they have decided to come into the store today is for Matt's situation concerning the erratic bus service. Lee is quick to point out how TopItUp can provide even greater peace of mind and convenience than other TopUp methods through the parental control feature via SMS. At the same time he points out to Mark that should he find himself in a similar situation with little or no credits, he can top it up via the 'Any Mobile' feature using a mate's handset. Mark is impressed and thinks that when the time comes he will try it from a friend's handset just to 'show off'.

John and Kristy are impressed with the benefits of the TopItUp service and are pretty much convinced that, coupled with their particular circumstances, topping up via SMS is the way to go, but want to know how to pay for the TopUps and what 'prepaid prepaid' means exactly.

Lee advises that John or Kristy (or possibly both) will need to sign a Direct Debit Authority (DDA) against their nominated cheque or savings account to pay for TopUps as well as completing the Registration Form as part of the registration process. Mark of course has his own bank account and can sign both forms for himself.

Customer Terms and Conditions

Lee takes them through the terms and conditions for using TopItUp. They understand:-

- that (like a contract handset) they are paying an upfront payment for the prepaid prepaid (initial) voucher (the TopUp Voucher value which is currently $30) to gain these benefits, however, the payment of this amount is a pre-purchase entitlement to something they own (being an entitlement to a TopUp Voucher for prepaid handset credits) and not a fee (unlike a contract);
- that by completing the Direct Debit Authority they authorise TopItUp to deduct the value of a TopUp Voucher from the nominated bank account to Register and whenever they Request a TopUp and that this authority applies if they were to order other products (such as ring tones) using TopItUp;
- that they agree to notify TopItUp promptly by phoning Customer Care if there are any changes to their financial institution account details;
- that there are sufficient funds in their account to cover the cost of the TopUp Voucher whenever they 'Request a TopUp' using TopItUp and that they are aware that their bank will charge them hefty fees if they don't have sufficient available funds;
- that an account will require up to three business days to pass between Requesting a TopUp to allow time for their funds to clear;
- that the personal information (including their bank account information) they provide to TopItUp when they register is secure and will remain private being used to allow TopItUp and any of its support agencies to conduct their account. The personal information will not be provided to or be used by any other organisation for marketing or any other purposes not specifically relating to the conduct of their account;
- that if they tick the 'Send Info Box', that they are giving their permission to TopItUp to send them SMSs from time to time to advise them of new services available with TopItUp;
- that they agree to keep their Password private. They should understand that giving someone their Password is akin to giving someone the PIN to their keycard account.
- that they pay for the cost of the SMS when they order a TopUp Voucher and that if they ring the Customer Care number on their mobile they will pay the standard mobile fee for a local call to an Optus 1300 number for each call;

- that TopItUp, at their discretion, may elect to close the Account.
- that should they decide to close their Account that TopItUp will SMS a final TopUp Voucher to their handset as long as
    - they have a pre-paid entitlement to a TopUp Voucher and;
    - their account does not have any bad debt provisions associated with the final TopUp Voucher.

Completing the Registration Form

Mark is going to signup with TopItUp on his own behalf. Lee provides a TopItUp Registration Form and a Direct Debit Authority form for Mark to complete. Mark's mobile handset number will be his account number. The T&Cs include a requirement that Mark agrees to have more than $30 (being the current TopUp value) available in his account whenever he Requests a TopUp. Mark understands that when he does Register, TopItUp is going to deduct $30 from his bank account that night and set this amount aside as a TopUp Voucher the next time he Requests a TopUp using TopItUp. Mark knows he has sufficient funds to cover the initial $30 Draw Down. Mark also thinks of a great password to protect his account. Since Mark is managing his own account, the Account Holder Name is entered as Mark Evans and the User Name is entered as Mark Evans. He writes this on the form for registration purposes with the knowledge that once it is entered into the system, he is the only person who can access his TopItUp account. Mark also wants to get ringtones for his handset, so he ticks the 'Send Info Box' that gives TopItUp permission to send information using SMSs when new services or specials are available to him.

Completing the Direct Debit Authority

Mark doesn't know his Direct Debit bank details. He does have his keycard with him. Lee has a current list of bank information handset numbers that allows him to quickly rings the bank's information number associated with the Mark's keycard and hands the handset over to Mark to get the details from his bank. Lee knows that recording this information is a very important step to get right so that the TopItUp registration process is not delayed. Mark selects 'Savings or Cheque' account option. Mark signs the Registration Form and the Direct Debit Authority Form thereby completing the instore registration process.

Kristy checks the credit balance on Matt's handset and finds that he has been more frugal than either Mark or herself. Matt has an available credit of $23.70. Lee explains that Kristy can manage Matt's account under her control. The Account Holder Name is entered as Kristy Evans and the User Name is entered as Matt Evans. She registers Matt's TopItUp account using all her other details including the direct debit authority with the debit card details of her own combined credit/debit card account details. Unlike Mark, Kristy does know her bank details as she makes payments to the electricity account using bPay. She does not want Mark getting ring tones or other promotion, so the 'Send Info Box' on the registration form is not ticked. She also picks a password that Matt or Mark cannot easily guess and signs the Registration Form and the Direct Debit Authority Form.

Kristy registers her own handset with the TopItUp Service. She enters her own name as the Account Holder and the User Name. She ticks the 'Send Info Box' keen to know about how to get the Bridge Over Troubled Waters ringtone that rings on Joanne's handset.

TopItUp User Guide

Lee also gives all three users a 'TopItUp User Guide' and explains each of the basic steps.

He programs the 'TOPUPS' number (0412 876877 or 0412 TOPUPS) into each of their handsets and makes sure Mark and Kristy know how to send an SMS with their Password to the 'TOPUPS' number as shown in the User Guide. He also tells them if they get into trouble to ring the 1300 TopItUp Customer Care number (**1300 300 482)** and also enters this number into the address book of their handsets.

Wait for Welcome Message SMS

Lee explains that they have to wait to get a notification by SMS from TopItUp before they can access their first TopUp Voucher. This is usually sent by TopItUp within 2 full business days. Business days do not include National Public Holidays. It is already well past the 4pm processing cutoff, which means that the Accounts may not be registered until Tuesday afternoon at the latest. If they had been in before 4pm, they would have made the daily cutoff and be registered before Monday afternoon.

The last thing Lee always does is to remind the customer that they will receive a Welcoming Message by SMS when they are registered which lets them know they can start to use TopItUp. He asks them not to send any Requests for a TopUp until they get the Welcome Message.

The Evans go home wrapped thanking Lee for all his help and knowing that they now have both control and the anywhere convenience that TopItUp provides.

John asks whether he could use his Master Card instead. Lee says 'no' as the service has been built around the overwhelming majority of prepaid users who are not credit card holders, and is the only way a prepaid user can avail themselves of the service. Besides, the merchant fees at the moment are too expensive. But he reassures John that in the future this payment method would most likely be available.

So what about the 'prepaid prepaid' part asks Kristy? Lee says that the TopItUp service is just like many other services people have where they pay in advance for the use of or access to that service. He puts it in terms of 'rental' fees as this is what most people understand about account services. Lee cites examples such as Telstra's monthly fixed-line access fees, electricity accounts, and Kristy's current Telstra mobile account which is just like Optus' contract mobile handset users who pay in advance and use up the access fee in included calls. Lee explains that TopItUp is different and better as the prepayment is actually for calls you can use and not a rental or access fee. In fact, he says, TopItUp charges no joining, ongoing or rental/access fees whatsoever.

Lee explains further that direct debits can take upto three business days to transfer the funds from their account to TopItUp. Once the funds are cleared, a TopUp can be ordered immediately requesting it by SMS. This starts the order process for the replacement TopUp which in turn will take upto three business days to transfer clear funds during which time another TopUp can not be ordered. John asks if they can get $50 vouchers. Lee explains the only vouchers that are issued are the $30 ones as there is no benefit to the customer to pay more if they can order when they need them.

Lee also explains the section in the User Guide that warns about having sufficient funds in the nominated bank account to cover the cost of the TopUp and points out that the banks will charge hefty funds if the account is overdrawn which will in turn delay delivery of the replacement TopUp. He puts forward the case that by prepaying now all subsequent payments can naturally be budgeted as spending with only monies you currently have available in your account.

This makes sense to Kristy and John, and, as they weren't sure how much they were going to spend on prepaid handsets today. They are happy to sign up.

Lee pulls out the Direct Debit Authority and Registration Form while asking for a copy of a driver's licence or best available ID. He photocopies the ID and commences to fill out the Registration Form first using that information to fulfil Optus' requirement for new customers connecting new or additional prepaid services. Lee is sure to complete every field in the Registration Form accurately and legibly knowing that the process demands the same attention to detail and integrity as do postpaid connections. He doesn't want to lose any revenue possibilities due to sloppy work .

Lee explains Kristy and Mark the importance of not providing your password to any other person. Kristy chooses a 4 to 6 character password for her own account and a separate one for Matt's account. Passwords should be letters and numbers and should not be whole words, such as FIDO, which are easy to guess. They can be typed in upper or lower case. The relevant password is written onto each of the Registration Form.

Once finished with the Registration Form, Lee now turns his attention to the Direct Debit Authority. John and Kristy have a joint bank account which they decided to provide the authority against. They state it's a savings account. Lee asks them first whether they have the BSB and account number for this bank account leaving the account name details to later. He's prudent enough to ask whether they have a cheque book just in case, as it would have all the necessary details.

They indicate that they don't have a cheque book for this account and don't know such details. Lee is not phased and simply asks for their financial institution's name and branch. They indicate that they are members of the Hornsby Teachers Credit Union as John has his wages paid into this account. As this is not one of the major financial institutions such as Westpac, CBA, ANZ or NAB and is not in the Wollongong telehandset directory area, Lee quickly goes to the web to access the contact handset number for the Credit Union. He

keeps a couple of browser applications open on his desktop, one of which is the WhitePages online website www.whitepages.com.au . He quickly types in the information he has into the appropriate fields and clicks 'search'. He checks with John that he has the correct institution and address and rings the number indicated. He hears the recorded message and realises that it is Saturday and that the credit union is closed until Monday.

Lee is not phased as he has secured John and Kristy's trust and they agree to sign the paperwork now and on Monday, Lee will ring John or Kristy for the BSB and Account Number details. Before the Evan's leave, he programs the TopItUp SMS Request Number (0417 866877) into each handset and stores it on their HandsetBook directories under the name TopItUp and makes sure they now how to send an SMS with their password to order a TopUp. He also programs the TopItUp Customer Care Number into their handsets.

Lee explains to them that once he has the bank account details and a successful debit of their account has occurred a Welcome Message with their password will appear on their handsets. Then, when they're ready to TopUp, use the TopItUp number stored in their handset to send the SMS containing their Password. He points out that the User Guide details all this but nevertheless if they have any problems to contact the Customer Care number.

After registering their handsets with Optus prepaid services, the boys are sending SMSs to each other that afternoon and to their friends. On Wednesday afternoon, Mark finds out that he can't make calls as he has run out of credit. As soon as he gets home, he rings Kristy at work and explains his problem.

Problem alright .... Kristy is not impressed. It's Mark's birthday tomorrow and he's spent $30 in four days. He needs to be taught a lesson but it is his birthday tomorrow. Kristy rings '555' to find out that she has $8 credit (after all, she did have to ring all her friends to tell them about her new mobile.) She didn't think she'd used so much. She's afraid to check Matt's handset. She rings John at work. John is not impressed either. John leaves for work early and gets home late. He doesn't know where to get TopUpand even if he did, he'd have to leave work 10 minutes early to get them and might miss his train. The milk bar near the railway station isn't open when he gets home. Disaster - Mark is without credit Wednesday night. He can receive calls so it's not a total disaster. Mark gets up early on his birthday to plead with his parents. They remember that Lee said you could get them just about anywhere and they remember what he said about TopItUp. Back to the store on Thursday night.

John buys Mark another birthday present being a $50 TopUp card over the counter with cash. Mark rings '555' and enters the voucher number purchased into his handset to restore his credit so that he can use his handset immediately.

Lee explains the best way to manage their handsets using TopItUp. The Evan's decide to signup.

TopItUp Dealer

Forwarding Registration Forms to TopItUp

Once the Evans family leaves the store, Lee faxes the completed registration and authority forms to TopItUp. Lee then stores the completed forms in a locked cabinet until they are mailed to TopItUp.

Once a week (on Monday), Lee mails last week's originals to TopItUp as required by the TopItUp Dealership Agreement.

Dealer Perspective

Lee is pleased to be able to help the Evan's and at the same time help his own store financially. By taking the extra trouble to mention TopItUp to them when they bought the handsets, they returned to his store when they needed the convenience that TopItUp provides.

Lee signed up his Network Communications dealership to become a TopItUp Dealer to stem the 'leakage' from his store of Prepaid customers. Lee knows leakage is occurring because a large number of the people who buy Starter Kits and Prepaid Handsets from him predominately buy TopUp cards from other outlets for customer convenience reasons.

The Evans were in store for 35 minutes to buy the handsets and 40 minutes to register all three accounts with TopItUp. Taking this extra trouble has made the Evans family valuable prepaid customers providing ongoing revenues of 12.0% to the store. Every time they order a TopUp using TopItUp, Lee gets this commission. Lee knows that the Evans have travelled from Port Kembla and even though he has provided exceptional after sales service, it is highly unlikely that he will see them unless they have a warranty problem or need a new handset. Assuming they are average prepaid users, signing each of them up will bring $43 in ongoing revenues every year which is better than the $6 he receives he would receive without TopItUp if he never sees them again.

True, this commission is not the full margin of an instore voucher but each commission is a payment that would not have occurred if the Evan's had bought elsewhere. Now, even if the Evan's go on holidays, move interstate or go to Australia Post, a service station or newsagent that sells TopUp vouchers, there is no reason they would buy a TopUp voucher from anyone else (unless they wanted a spare voucher).

The store opened just over twelve months ago and the number of vouchers and starter kits sold each month grew for 9 months and is now starting to level off. Whilst Lee knows that his store is capturing a significant

number of sales of prepaid handsets and starter kits sold in Wollongong, he is selling approximately four times this number of TopUps month after month. This means his potential for revenue is 'leaking'.

Lee had been shown figures that if he started selling TopItUp from day one registering just 25% of prepaid customers coming in store he would be able to stop the 'leaking of his prepaid customer base'. Lee knows it is in the best interest of his store to aggressively push TopItUp to every prepaid customer entering his store convinced that the 'Best of Both Worlds' applies not only to customers but to dealers as well.

Other Dealer Opportunities

Lee wonders if he can't use the store promotion code to sign up Marks' local football club after Mark makes a comment about how many of his mates at footy think TopItUp is brilliant.. A lot of the members are juniors, about half of which own prepaid mobiles. Lee thinks, I could approach the Club Committee and offer them a fund raising opportunity. For every person signing up to TopItUp, I could donate $1 of my commission on every TopUp voucher ordered through the club. Lee understands that he is giving away some commission, but he is gaining revenue from an audience that might never enter his store. Better still, some of the people signing up may be Telstra or Vodahandset users.

Mark gets the Secretary of the Club to ring Lee. Andrew had just been working out whether 'its chocolates or cookies' this month as the club fundraiser. When Lee explains that Andrew only needs to have one fundraiser that is ongoing and doesn't take up any of his time, he is enthusiastic. He asks Lee to give him some brochures to present at the next Club meeting and asks 'Would you be prepared to come to the following meeting? Can people go to your store to sign up?'

Lee knows he can produce the payment information from the reports he gets from TopItUp to write ongoing monthly cheques to the Club as the best money raiser they've ever had.

Best of Both Worlds all right thinks Lee for churches and clubs as well..

Dealer Obligations to TopItUp

Lee completed a Dealer Registration Application for a TopItUp Dealer Agreement which includes obligations on the Dealer to honestly represent TopItUp to potential prepaid customers and act with integrity in dealing with TopItUp customers and TopItUp. The Dealer Agreement is renewed annually.

The Dealer Agreement applies obligations on the Dealer to ensure

- that the Dealer prominently displays TopItUp's Privacy Statement and understands his role in the privacy obligations as an agent of TopItUp;
- that the customer's Personal Information is subject to TopItUp's Privacy Statement;
- that the customer understands TopItUps Terms and Conditions;
- that the customer has been adequately walked through the TopItUp User Guide;

- that the bank account details provided by the customer are complete and accurate either by witnessing documented evidence provided by the customer or by information provided when the customer handsetd their bank's information line in store;
- that customer Registration and Direct Debit forms are completed accurately, signed and forwarded to TopItUp as required;
- that the customer's handset has been programmed with the TOPUPS number and the TopItUp 'Customer Care Number'.
- that the Dealer has an ABN and invoices TopItUp using this ABN for commissions paid including GST.

TopItUp Obligations to Dealer

The Dealer Agreement applies obligations on TopItP to support the Dealer in the following manner:-

- Dealer Support for Lee is provided by TopItUp. TopItUp provides a Dealer Manager who also performs the role of TopItUp's Privacy Officer. Dealers would handset the Dealer Manager in the first instance for all support issues;
- Dealer is required to display TopItUp branding for the period of the Dealer Agreement;
- Provide up todate collateral and point of sale material to the Dealer ;
- As a dealer, Lee receives commission advises by email daily showing month to date commission and commissions pais in the previous 24 hour period.
- Once a month, TopItUp will provide a Monthly Commissions Report to the Dealer showing all the ongoing transactions processed within that month for that Dealer;
- The Dealer is to invoice this amount (inclusive of GST) and fax/email this invoice to ensure prompt payment and followup with the original invoice in the mail.
- Upon receipt of fax/email, TopItUp will make a monthly commission payment direct to the Dealers bank account.

TopItUp also provides useful management reports to the dealer on a month by month basis in a format that can be imported into an Excel spreadsheet and used for in store sales analysis.

Dealer End of Term

The Dealer Agreement is renewed annually by TopItUp. The Dealer Agreement provides for ongoing commissions to a Dealer from the TopItUp customers signed up by the Dealer for the currency of the agreement.

There are four sets of circumstances under which the Dealer Agreement would or could be cancelled or terminated being:-

- Initiated by Dealer – under these circumstances would normally cease and the customers signed up from the dealer may be reallocated. At the sole discretion of TopItUp, commissions may be continued to be paid to a bank account nominated by the departing dealer;
- Dealer sells dealership – under these circumstances, the new dealer would be allocated a new dealership account (consistent with Optus Dealership code) and the customers associated with the old dealership will be paid to the new dealership. This is achieved by the bank account details of the old dealership being changed to reflect the new dealership bank account details and the new dealership would receive two commission payments (one for the old account number and one for the new account number). The customer base is effectively split over both the old and the new account code. TopItUP will not allow customers to be registered to the old dealer account;
- Initiated by Optus or Network Communications – if the dealer is no longed authorised by Optus Communications or Network Communication to be a dealer, the TopItUp dealership will be automatically terminated;
- Initiated by TopItUp – if the dealership has acted inappropriately in the interests of TopItUp, the dealership will be terminated and ongoing commissions to the dealership will not be recognised.

Back Office Staff Roles

TopItUp is administered and operated by the following staff categories performing roles that provide appropriate security access controls to perform their operational responsibilities:-

- Scheme Operators – perform all the back office registration functions for TopItUp ensuring the completeness and accuracy of information is correctly entered, that the initial 'Draw Down' of funds is completed correctly, that Bad Debts and Bad Bank processing of preRegistered accounts is handled correctly and that Accounts are Activated correctly.
- Scheme Administrators –have full access to all of the operational management functions of the System and perform financial and settlement administration, customer complaint resolution and fraud management of the system.
- Financial Administrator - is responsible for the Financial Management of TopItUp including the financial management of the company with specific responsibilities for internal audits of the System and oversight of payment and settlement functions.
- Customer Care Operator – perform all Call Centre functions for calls received by TopItUp through the 1300 Customer Care number. **(1300 300 482)**
- Dealer Manager – overall responsibility for dealer management including dealer appointments, dealer training, dealer support, complaints resolution and dealer collateral.
- System Administrator – overall responsibility for IT Systems, support, disaster recovery and security.
- Software Support – provided by Fieldware Pty Limited.

Staff Type – Scheme Operator

On Friday morning at 9am, Ann makes her first coffee of the day. She is one of TopItUp's Scheme Operators and is responsible for the back office registration functions for TopItUp. Ann knows it is important that she ensures the completeness and accuracy of information is correctly 'Registered' and that the initial 'Draw Down' of funds is completed before Activating the TopItUp Account.

Stopping near the fax machine, Ann draws off the faxes received for the Evans family (amongst others). Ann logs into TopItUp's Backoffice system with access rights to create and update account registration details and to Activate Accounts. Ann creates Accounts for Mark, Matt and Kristy entering their details into the TopItUp backend system. She checks all the paper work carefully. If there any problems, such as a customer not completing all required information or signing either form, she will handset the customer directly. She double enters the Password field and the bank account fields to ensure a system accuracy check of this information.

When Ann has completed the data entry for each Account, she saves the registration details which sets the state of the Account to PreRegistered and will commence the Initial Draw Down process.

Three things will now occur. Either

- The applicant's Initial Draw Down fails because of a declined payment by their bank
- The applicant's Initial Draw Down fails because of a incorrect BSB or account details
- The applicant's Initial Draw Down is settled and the Account is Activated.

SO - Follows up Initial Bad Debt

Ann does the follow up of any Bad Debts associated with new users registering to TopItUp. Ann prints a PreRegistered Payment Exception Report which shows her all accounts that have failed the Initial Draw Down of funds for the reasons of Bad Debts (payment declined) or Bad Bank account details (rejected account details).

The Report is sorted in reverse date order so Ann can start at the top of the Report and find the Accounts that have failed activation most recently. Ann knows it is important to keep the customers confidence and that this hiccup, if overcome, will ensure the highest rate of ongoing customer satisfaction with minimal cost impact to the customer and TopItUp.

Ann will handset the Account Holder directly advising them of the payment decline or bad bank details. Ann informs them that their account cannot be activated until the payment can be cleared or the bank account details made accurate.

If there has been a payment decline (indicated by TopItUp declaring the state of the Account as PreRegistered_BadDebt), Ann will also inform them that their bank will charge them a dishonour fee. Ann

asks them to handset the TopItUp Customer Care number when sufficient funds haven been deposited to cover the TopUp Voucher and the dishonour fee from the account holder's bank. Summary notes are entered against the Account. No other action is taken until the Account Holder handsets back. The payment process is then repeated. If the payment is declined a second time, in most circumstances, the Account would be cancelled by an Scheme Administrator. TopItUp absorbs the merchant dishonour fee of $2.50.

SO - Follows up Initial Bad Bank

If their BSB or bank details have not registered (usually notified on the first overnight settlement and indicated by TopItUp declaring the state of the Account as PreRegistered_BadBank), Ann will handset the Account Holder explaining what has happened and ask for them to fax details of their bank account details (eg a current statement) to TopItUp to allow their correct bank details to be entered. Summary notes are entered against the account. No other action is taken until the Account Holder faxes the details.

When the fax is received, Ann will file the proof of account faxed by the account holder with their registration forms and update the Account with the correct bank accoiunt details and set the state of the account to PreRegistered which will restart the Initial Draw Down..

SO - Initial Draw Down is Settled

TopItUp performs automatic settlement (with provision of manual override) of settlement of Draw Downs after a maximum of two business days.

If an Account has not failed the Initial Draw Down by either of the above reason, TopItUp will automatically Activate their Account which will automatically generates a Welcome Message to the Account handset, allocate an entitlement to a TopUp Voucher (known as a PIN by transferring an unallocated PINs to the Allocated PIN Pool associated with the Account Holder's Account. As part of the end of day settlement process, a commission notification email is sent to the dealer known as a Daily Dealer Commission Notification associated with the Account notifying them the Account has been Activated and notifying them of their commission entitlement. The Notification also details the settlement transaction details including the name, account number and the commission amount and customer activity (registration activation or top up).

Staff Type - Scheme Administrator

Joe is a Scheme Administrator for TopItUp. He has full access to all of the operational management functions of the System and performs

- customer complaint resolution
- operational fraud management of the system
- cancelling customer accounts associated that are not initiated by the Account Holder
- acquirer bank settlement functions including
    - preparing Bank Bulk Funds Movement files
    - receives Bank Settlement Files

- manual oversight of closing open settlement batches as required

SA - Morning Settlement

Each morning, Joe accesses the TopItUp's online bank account from its acquiring bank and exports this information to a Bank Settlement File. The Bank Settlement File shows all batches that were Closed and those that remain Open from the previous evening's settlement by the acquiring bank

TopItUp performs a sophisticated clearing process whenever an Scheme Administrator runs the Process Account Statement option. Batches are either Open or Closed.

When a batch is Closed, TopItUp knows that every customer transaction in the batch has been accounted for as either cleared (payment received), not cleared (a bad debt) or not processed (a bad bank) by the acquiring bank.

Settlement Batches processed by TopItUp's acquiring bank Joe then imports the Bank Settlement file into TopItUp and runs the 'Process Account Statements' option. This option processes all reports and updates the Account as a result of the Settlement process.

SA - Afternoon Preparation

TopItUp's acquiring bank has a 5pm close off. Joe runs the Prepare Bulk Funds Movement File option which prepares a file to be uploaded to the acquirer bank. This option will include all Draw Downs that have been generated since the option was last run. The file breaks the Draw Downs into settlement batches of 100 (configurable) entries per batch.

Joe uses application software provided by the acquirer bank to upload the Bulk Funds Movement File.

Staff Type – Financial Administrator

Morgan is the Financial Administrator for TopItUp. He is responsible for the Financial Management of TopItUp including the financial management of the company with specific responsibilities for internal audits of TopItUp and oversight of payment and settlement functions. He is also responsible for authorising and purchase order approval for TopItUp to order additional PINs to replenish the Unallocated Pool with replacement TopUp vouchers from the voucher supplier when the Unallocated Pool quantities fall below the just in time re-order point.

Staff Type - Customer Care

Craig is a Customer Care Agent and works in TopItUp's call centre. Craig is trained in handling most customer scenarios and will only pass a call onto an Scheme Administrator in the event of a Customer Compliant.

Craig knows the importance of identifying the Account Holder or the Account User as appropriate.

Craig normally accesses and Account by the Account Number being the mobile handset number associated with the Account. Craig can access also an Account Holders details by a surname search against the Registration Database and further qualification of the Account Holder.

Whenever Craig takes a call from a customer, he is aware of TopItUp's obligation for confidentiality of the Account Holder's private information.

Craig will type a record of the conversation which is attached to the Account and is known as a 'File Note'. File Notes are date and time stamped and identify the Customer Care Agent and record an outcome for the interaction with the caller.

Back Office Scenarios

Applicant Fails Registration

Mark is not having much luck. On the following Monday, Mark's name appears as declined on the PreRegistered Payment Exception Report as a declined payment. Ann rings him and requests that he checks why his payment is declined. Ann asks him to ring back on the TopItUp Customer Care 1300 Number when he has deposited sufficient funds to clear the bank decline fee and the amount of the TopUp Voucher. Ann gives him a call log number to quote that is generated from her system and types in details of their conversation.

Mark is embarrassed and thanks Ann for letting him know. He has not decided whether to tell his mum or forget about TopItUp. Mark eventually tells Kristy.

If Ann hadn't been able to contact him, she would have sent an SMS to Mark asking him to call Customer Care and quote the call log number. TopItUp has already changed the processing state of Mark's account from 'PreRegistered' to 'PreRegistered_BadDebt'. Changing the processing state to PreRegistered_BadDebt means that whenever an Scheme Adminstrator (such as Joe) or an Scheme Operator (such as Ann) runs the PreRegistered Payment Exception Report, Mark's name will appear. At some point in time, Joe would assess this account is not likely ever to be registered and Cancel the account by changing the state of the account to 'Cancelled'. Ann (being an Scheme Operator) does not have access to perform this function.

Applicant is Activated

On the Tuesday morning, Kristy and Matt's accounts are Activated. This means that $60 was drawn down from Kristy's bank account on Friday night has cleared and that A 'TopUp Voucher entitlement has been automatically allocated to both accounts.

Customer gets a Welcoming Message to TopItUp

When TopItUp Activates Kristy and Matt's accounts, TopItUp sends a Welcoming Message to both handsets stating "Welcome to TopItUp. You can now Request a TopUp. Thank you for using TopItUp"

Dealer Commission Advise

The commission advise for Kristy and Matt's initial TopUp is automatically processed at the end of day settlement run on Tuesday and a settlement advise is generated and emailed to Lee showing details of the commission and the activities that generated the income.

Lee rings Kristy after seeing that Kritsy and Matt have been Activated on his report. He asks if she has any questions. Kristy thanks Lee and says she will recommend TopItUp to her friends.

Need Sufficient Funds to Re Register

When Kristy gets her SMS notifying her that her account has been activated, she remembers about Mark's decline. She was going to let Mark stew until he could fix his bank account balance. She rings John and they agree to cover Mark's funds and John deposits the required funds into Mark's bank account using internet banking.

When Matt gets his Welcome SMS, he rings '555' to check his account balance to see if he needs to use TopItUp. He then remembers that he can't use the service as he doesn't know the Password. He thinks 'maybe I can get mum to tell me'.

Kristy then rings Matt to see if he received a Welcome SMS as well. Matt asks for the Password but Kristy tells him to wait at least 6 months until he proves that he can be trusted. Matt straight away blames Mark for creating problems himself without understanding that if Kristy gives him the Password, he has open slather on Kristy's bank account.

John rings Mark to tell him that he deposited the required funds into his account to try to reactivate his account with TopItUp. Mark thinks this is brilliant news, he has almost run out of credit. John also tells Mark that once he is registered, that he cannot request a TopUp Voucher until Mark has deposited sufficient funds to cover the bank fee and the TopUp Voucher into his bank account. This is not good news for Mark.

Mark Calls Customer Care

When Mark gets home from school, he rings the TopItUp Customer Care number using the home handset. Craig is a Customer Care Agent and works in TopItUp's call centre. Craig is trained in handling most customer scenarios and will only pass a call onto an Scheme Administrator in the event of a Customer Compliant.

Craig takes Mark's call asking for Marks handset number. Craig accesses Mark's account. Craig then asks for his name, current address and date of birth. Craig verifies that Mark is the Account Holder. Craig also sees from the file note that Mark's account is 'PreRegistered_BadDebt'.

Craig asks how he can help. Mark says that he has put money into his bank account as requested and can you try to activate my account please? Craig explains that this is the second attempt at registration and that since it is Wednesday, expect a Welcome SMS on Friday saying that the account has been activated. Mark agrees and Craig enters a File Note and changes the state of the account from PreRegistered_BadDebt to PreRegistered.

Craig asks if there is anything else he can do to help. Mark says no and rings off.

Mark's Account is Ready for Second Registration Attempt

When Joe runs the Create Bulk Funds Movement File option at 4:30 pm that day, Mark's second attempt at registering with TopItUp is included in one of the settlement batches uploaded to the acquirer bank. On Friday morning, the batch that contains Mark's settlement is Closed, TopItUp determines that Mark's funds have cleared and Mark's Account is Activated by TopItUp. Like Kristy and Matt one week before, Mark now receives an SMS welcoming him to TopItUp and his entitlement to a PIN is made.

Other Registration Problems – Account Number is Not Accurate

In this scenario, the Customer's handset number (their account number) is not registered accurately. This could be caused by the number not being recorded accurately on the registration form or incorrectly entered into the Schemes database when registering. The chance of the second reason is minimised as the SO is required to re-enter the account number to verify the entry.

In either case, the fact that the account number is not recorded correctly is a problem as the Customer will not receive a 'Welcome Message' to the scheme as the SMS will be sent to another prepaid mobile number.

The following scenarios may occur:-

- If the incorrect mobile number is not registered on the carrier's network, the System will know something has gone wrong and the System will generate an exception report to be investigated by an SO. A letter may need to be sent to the Account Holder requesting the Account Holder to ring an SO direct and not Customer Care.
- If the number is registered on the carrier's network, the Welcoming Message will be sent to another mobile handset. This certainly presents a problem. TopItUp believes the account is registered and the Account User is still awaiting their Welcome Message. This registration will remain in an error state until the customer eventually rings Customer Care who do not have a record of the account number being quoted by the customer. Customer Care will need to locate the account using search features and referring the matter to an SA.

Other Registration Problems – Account Number is Reissued by Carrier

In this scenario, the Customer's handset number (their account number) has been reissued by the carrier after the number has been cancelled and quarantined by the carrier. This presents a problem if the previous user was also registered with the Scheme as an account associated with that number exists in the System.

When the SO attempts to register the new account, the SO will be aware the old account exists and will alloacate a two digit suffix (starting with '00') to the old account number. This action will identify the old account as superceded yet still tied to the old account number and then allow the new account to be established.

TopUp Scenarios

Kristy Requests a TopUp for Her Account

Later that month, Kristy decides to Request a TopUp. She goes to the SMS messaging area on her handset and writes an SMS containing her Password only. She finds the number for TopItUp that Lee saved on her handset and sends the SMS. *She remembers that Lee had asked her to delete the sent SMS from her handset for security reasons and does so.*

The TopItUp system receives her request and processes the request within a minute of the SMS being received. Processing the request will select the oldest PIN activation date from the $30 Optus TopUp Pool and sends that PIN as the TopUp Voucher using an SMS to Kristy's mobile handset. If the Reward System is running, Kristy would also get an acknowledgement of the Reward Points due.

Kristy gets her TopUp Voucher from TopItUp

Kristy remembers that Lee had told her that the TopUp process in most instances is pretty much immediate. He pointed out to her in the User Guide that if there were problems with the SMS network, such as network congestion or coverage for her handset, delivery will be delayed. If she hasn't received the TopUp Voucher within the hour, she should send another SMS to re-request the voucher.

Kristy receives an SMS with her TopUp Voucher within two minutes. When she reads the SMS, the message is "Your TopUp Voucher is 1234567890. You have 25 TopUp Points. Thank you for using TopItUp". She reads the SMS and writes down the TopUp Voucher number. She rings '555' and enters her TopUp Voucher as if she had purchased it from a store.

TopItUp starts a Draw Down on Kristys' Bank

TopItUp will then start the Draw Down process on Kristy's bank account for a replacement voucher. TopItUp automatically changes Kristy's account state from Active to Pending. Overnight, TopItUp requests the Draw Down from Kristy's bank. At the completion of At the same time that TopItUp will automatically

change the state of Kristy's account from Active to Pending, meaning that TopItUp has started a Draw Down process of additional funds from Kristy's bank account.

Clearing is performed by exception. Unless the account is declared a Bad Debt, after two business days, it is assumed the payment has been cleared which will change the state of the account to Active and a PIN is transferred from the unallocated PIN pool to the $30 Optus allocated PIN pool. This completes the Draw Down.

Kristy Knows Not to Send Multiple Requests

The User Guide also points out to Kristy that if she was to resend the Request a TopUp within 24 hours of her first request, TopItUp will send back the same PIN that was sent on the first request plus a message saying this is the second notification.

This allows the user to get the TopUp Voucher again if they didn't receive it, were too impatient or lost the number before entering it into the handset.

A third request will likewise resend the TopUp Voucher. The SMS to the customer indicating this is the third and final transmission of the same PIN.

TopItUp will not send any further SMSs and will effectively ignore any further SMS received from the account until the funds have been drawn down and a new TopUp Voucher is available to be requested. If the customer handsets Customer Care, the system will provide sufficient information to allow the Customer Care Operator to explain the state of their account.

User Problems - Bad Attempts

'Bad Attempts' are attempts to Request a TopUp that cannot be processed by TopItUp for whatever reason. They can occur by accident or could be the result of a fraud attempt.

In the following scenarios that generate Bad Attempts, TopItUp always writes the full contents of any SMS received that generates a 'Bad Attempt' to the 'Potential Fraud Log File' in the event that fraud is being attempted on the system.

In some of the scenarios listed, the account will be flagged as 'Blocked' which means that TopItUp will not issue TopUp Vouchers to a Request a TopUp from the account, nor will TopItUp send other SMSs to the account. Blocking an account does not stop TopItUp's automatic processing of account states. performed by TopItUp in Accounts can only be 'Unblocked' by an Scheme Adminstrator.

Matt attempts to guess the Password

Matt attempts to Request a TopUp guessing the Password that Kristy created for his handset. He types in their dog's name as the password and sends the SMS to TopItUp using his handset.

When TopItUp receives the SMS, the system verifies Matt's account is is registered with TopItUp but the Password sent does not match the entry in the TopItUp database. TopItUp sends an SMS to Matt's handset which informs the user "Bad attempt, your Password is not correct. If you get it wrong again, call 1300 TOPUPS". *The state of the account is 'Active'.*

Matt panics. He calls 1300 TOPUPS on his mobile. He speaks to George from the TopItUp Customer Care Centre. George asks how he can help. Matt says that he has forgotten his Password, can you help. George asks for the Caller's name. Matt gives his name. Other questions would normally follow but George notices that Matt is the Account User and not the Account Holder. George informs Matt that the Account Holder (without identifying the Account Holders name) must contact TopItUp in person. A record of conversation is made.

Matt is not one to give up easy, maybe the Password is Kristy's favourite colour. He's not sure what to do. If he gives up and Kristy performs the next TopUp Voucher on Matt's behalf and gets the Password correct, the Bad Attempt logic is broken and the account will operate as normal.

Matt decides to risk it two days later. Even though two days has passed, TopItUp remembers his first bad attempt. He enters the Password as 'blue' and sends his second SMS attempt to crack the Kristy's Password to TopItUp. When TopItUp cannot validate the password on the second attempt, TopItUp assumes fraud and flags this account as 'Blocked'.

Two Bad Attempts are allowed before the account is automatically Blocked. One SMS is sent in response to the first Bad Attempt. This must be dealt with by an Scheme Adminstrator.

The Result is Matt's Account is Blocked

When an account is Blocked, no further TopUp Vouchers or SMSs will be sent to the account handset and all SMSs received are written to the 'Potential Fraud Log File'

Matt does not tell Kristy he has attempted to crack her Password. A Customer Care Operator accepting a call from an Account Holder with a blocked account will forward the call to an Scheme Administrator who determines whether a fraudulent attempt has been made to access PINs.

Kristy makes two attempts to request a TopUp Voucher without receiving any replies from TopItUp. Eventually Kristy calls Customer Care to report the problem. Kristy is passed through to Joe who determines that Kristy is the Account Holder by asking her personal details and verbally verifying her Password. Joe

informs her that there have been three recent attempts to request with bad passwords followed by two attempts with correct passwords giving her the date and times. Kristy verifies the two most recent attempts were hers. She is horrified when Joe tells her that a caller identifying themself as Matt had handsetd to ask for the Password.

Joe is satisfied that while a fraudulent activity has occurred, that it will remain in the family and that the account can be Acivated which he does. He records the converstion against the account. Kristy can now request a TopUp Voucher.

Unregistered user attempts to use TopItUp

Greg (Mark's friend) tells his father about TopItUp. Greg hasn't been to a Network Store. His dad had just bought him a Optus Prepaid Starter Kit from the Post Office. Greg has seen Mark request a TopUp Voucher. He puts his PrePaid Sim into his father's handset and sends an SMS to TopItUp's SMS number using Mark's Password. He knows Mark's Password, after all Mark had been told not to give out his Password, but, after all, Greg is his best mate.

When TopItUp gets his SMS, TopItUp does not have an account for the Greg's mobile number and sends back an SMS to Greg's handset informing him "You must Register your handset to use TopItUp at your nearest Network Store or ring 1300 TOPUPS". TopItUp records his handset number in case he decides to send additional requests before Registering with TopItUp. If any subsequent SMSs are sent by Greg, TopItUp will write these attempts to the 'Potential Fraud Log File' to be investigated by an Account Administrator for potential fraud. No further SMSs are sent by TopItUp.

Greg goes to a Network Store and signs up to TopItUp. When his account is Registered on TopItUp's Customer Base, any logic that TopItUp used in dealing with Unregistered Attempts made previously by Greg is broken and Greg's account is conducted normally.

One Bad Attempt is allowed by a user attempting to use an Unregistered Handset. One SMS is sent as a response to the first Bad Attempt. Subsequent SMS received from the same handset are automatically logged to the 'Potential Fraud Log File'. TopItUp will also create an entry for the mobile used to initiate the SMS in the 'unregistered handset database' maintained by TopItUp and will maintain logic regarding additional 'Bad Attempts' from this handset.

Any Mobile Scenarios

'Any Mobile' is an advance feature that allows a TopItUp user to use any other mobile to send an SMS to TopItUp to request a TopUp in the event that the user's handset does not have sufficient credit to send an SMS. TopItUp requires that any mobile that sends a Request a TopUp to TopItUp is to have the handset setting for 'Caller ID' to be switched ON. This applies to Any Mobile scenarios as well.

Kristy sends a TopUp Voucher to Matt using 'Any Mobile'

There are two ways Kristy can use TopItUp to provide a TopUp Voucher to Matt.

The first method requires Matt to give Kristy his handset. Normally, Kristy would TopUp Matt's handset for him by simply grabbing his handset and sending a TopUp request using the password she created for Mark, sending the SMS and deleting the sent SMS from Matt's handset.

However, Matt has gone to camp and Kristy cannot access his handset. Matt is still trying to work out how he can get the password to his TopItUp account. He rings Kristy asking Kristy to provide the password so that he can TopUp his handset himself. Kristy remembers that the TopItUp User Guide explains how she can send a TopUp Voucher using the 'Any Mobile' feature of TopItUp to Matt without having access to his handset. The User Guide says "Type in the Password, then a space and then the TopItUp Account Number eg 'PASS 0412123456' ". Kristy writes an SMS on her handset. She types in Matt's password followed by a space followed by Matt's mobile handset number. She sends the SMS. The User Guide informs Kristy that she has a maximum of two tries to use 'Any Mobile', so she is careful to make sure the Password and Matt's Mobile Number are correct and are separated by a space.

When TopItUp receives her request, it reads the password supplied and verifies the password against the 10 digit handset number following the space. *Any additional spaces entered in the handset number are ignored.* They match, so TopItUp sends an SMS to Matt's handset with the TopUp Voucher as if the request were sent from Matt's handset. Matt reads the SMS and enters the TopUp Voucher number after calling '555'. Meanwhile, TopItUp places Matt's account as pending and starts the Draw Down on the bank account details provided by Kristy (as the account holder) when she registered Matt's handset.

Mark runs out of Credit and uses 'Any Mobile'

Mark has gone out on Friday night and is using his handset to contact friends deciding where to go. He dials Jenny, he hears a prerecorded message telling him to TopUp before making this call. He tries to send an SMS and finds the same problem. He remembers that he can he can still use TopItUp if he can get a friend to allow him to use their handset to send an SMS. Greg has his dad's mobile which uses a Telstra postpaid account . Mark uses Greg's mobile to send an SMS to TopItUp. Mark punches in his Password followed by a space followed by his handset number. He sends the SMS. However, his Password is not correct.

Bad Attempts Using 'Any Mobile'

For security reasons, when TopItUp checks the password against the account number provided in the SMS (sent as Mark's handset number), TopItUp sends an SMS to Mark's handset informing him "This is your first attempt using 'Any Mobile' and the password entered is incorrect". TopItUp also writes an entry into Mark is excited when his mobile gets the SMS from TopItUp. He reads the SMS and is dismayed that the Password he entered is wrong.

Mark forms another SMS on Greg's handset and tries again. This time when TopItUp receives the second request it knows this is the second attempt using 'Any Mobile' from the same handset. Mark gets the Password right but gets his own handset number wrong by missing one of the digits. When TopItUp received the SMS it can't find a match for the account number to verify the password. TopItUp registers this is the second bad attempt from the same 'Any Mobile' handset. Only two attempts are allowed using the 'Any Mobile' feature from the same handset. TopItUp will not respond by sending an SMS on the second attempt or subsequent attempts from the same handset and writes the details of all attempts from the same handset using the 'Any Mobile' feature to a logfile that is reviewed by Joe or another Scheme Administrator as a potential fraud attempt or a denial of service attack.

Had Mark not entered his handset number correctly on the first attempt, TopItUp would have sent the notification SMS to Greg's handset as the Account Number could not be verified. The SMS sent would inform him "This is your first attempt using 'Any Mobile' and the Handset Number entered is incorrect."

Mark is out of luck again unless he uses another friends handset or a TopUp voucher from a store.

Two Bad Attempts are allowed by a user attempting to use 'Any Mobile' using the same mobile handset. One SMS is sent as a response to the first Bad Attempt. Subsequent SMS received from the same handset are automatically logged to the 'potential fraud log file'. TopItUp will also create an entry for the mobile used to initiate the SMS in the 'unrgeistered handset database' maintained by TopItUp and will maintain logic regarding additional 'bad attempts' from this handset. Since the bad attempts do not originate from the account holders handset, it is not appropriate to Block the account.

Account Holder wants to Close Account

Closing an account by a customer request involves the Account Holder calling a Customer Care Officer who has the authority to close the Account requiring the Account Holder to supply the Password to verify the action. Once the Account is Cancelled any additional SMSs sent to TopItUp for this account are logged in the 'Potential Fraud Log File' and no other action is taken by TIU. TIU retains all transactions and file notes associated with Cancelled Accounts for database integrity reasons but only an SA and an FA can view the Personal Information.

If a CCO receives a call from someone claiming to be the Account Holder of a Cancelled Account, the CCO can only verify that the Account Holders name, the Account Number and the fact that the Account was closed on a specific date. Only an SA or an FA can reactivate a Cancelled Account.
The following scenarios apply to an Account Holder closing an Account.

Active Account is Cancelled – Send TopUp by SMS

Matt keeps bugging Kristy for her Password. Kristy thinks enough is enough and decides to close Matt's account. She rings George at Customer Care. After George has identified Kristy as the Account Holder to Matt's Account, Kristy asks George to close the account. *Had Matt handsetd and tried to close the account, George would have identified Matt as the Account User and told Matt that only the Account Holder can close the account.*

As a CCO, George through five steps to close the account.

- STEP 1 - He asks Kristy for her Password and enters it into the 'Confirm Password Entry' box on his screen. *The Confirm Password Entry box must be completed successfully for a CCO to either change the Password on an Account or to Cancel an Account.*

- STEP 2 - George asks Kristy if she doesn't mind telling him why she is cancelling the account. George has a number of codes that summarise why an Account may be closed which are

Code	Reason for closing account
1.	Customer doesn't need the service anymore
2.	Customer handset has been stolen
3.	Customer dissatisfied with service – delivery of TopUps
4.	Customer dissatisfied with service – bad encounter with dealer
5.	Customer dissatisfied with service – bad encounter customer service
6.	Customer dissatisfied with service – problem with bank
7.	Customer – other eg privacy, security concerns
8.	TIU SA - Customer has attempted to defraud system
9.	TIU SA - Customer has incurred too many bad debts
10.	TIU SA – Customer is PreRegistered_BadDebt for too long
11.	TIU SA – Customer is PreRegistered_BadBank for too long
12.	TIU SA – Customer's account considered dormant
13.	TIU SA - Other

When Kristy explains, George sees this as a customer who has security concerns and enters a Code 7 with the file note. *George only gets to see Reasons 1 to 6 on his entry screen as they all relate to customer initiated reasons for closing the account. An Scheme Administrator would use Codes 8 to12 only to Cancel an Account.*

- STEP 3 - George checks the State of the Account to determine the Account Holders entitlement to a TopUp Voucher. George can only issue a TopUp Voucher immediately if the State of the Account is Active. The State is Active, so George knows Kristy is entitled to a TopUp Voucher and informs

Kristy of her entitlement and that TopItUp will SMS the TopUp Voucher to Matt's mobile. Kristy agrees, so George Cancels the Account using the 'Cancel with SMS Option' which changes the State of the Account to Cancelled, SMSs the TopUp Voucher to the Account's Mobile with the message "You have requested your account be closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp. You can rejoin" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 4 - George tells Kristy the TopUp Voucher is on its way and that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

- STEP 5 – Kristy receives her TopUp Voucher entitlement by SMS. Any additional SMSs sent to TopItUp are logged in the 'Potential Fraud Log File' and no other action is taken by TIU.

Active Account is Cancelled – Send TopUp by Mail

Had the State of Kristy's Account been Active but she could not or did not want to receive her TopUp Voucher by SMS, George would sent it by Mail. Steps 1 and Step 2 are repeated as above.

- STEP 3 (CCO) - Kristy may have told George that Matt's had been lost/stolen or that she just doesn't want the TopUp Voucher sent to the Account's Mobile. In these circumstances, George would have have checked Kristy's address details and then used the 'Cancel with Letter' option which changes the State of the Account to Cancelled, prints a personalised letter to Kristy as the Account Holder informing her '*You have requested to have her account closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp and you can rejoin at any time by calling Customer Care on 1300 TOPUPS*" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 4 - George tells Kristy the TopUp Voucher is being mailed and that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

- STEP 5 – George then mails the letter with the TopUp Voucher number to Kristy's address.

Pending or PreRegistered Account is Cancelled

Had the State of Kristy's Account been Pending or PreRegistered when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

- STEP 3 (CCO) - George would have explained to Kristy that TopItUp was clearing funds with her account. As a result he can start the process of closing her Account which will not allow further

TopUp Vouchers to be requested or delivered. When the funds are cleared, TIU will mail your TopUp Voucher to you. Kristy agrees.

In these circumstances, George would have checked Kristy's address details, Updates the File Note and used the 'Cancel with Letter Option'. This time the letter does not print and cannot therefore be mailed. When the State is Pending, this action flags the Account as 'Blocked' which allows TIU to complete the Draw Down and at the same time disable the Account from sending TopUp Vouchers or replying to SMSs sent by the customer.

- STEP 4. George tells Kristy that should she desire to reactivate the Account, please handset Customer Care. Thank you for using TopItUp.

TIU has not Cancelled the Account. Blocking the Account means that whenever an SA runs a Blocked Accounts Report, Kristy's account will show.

As an extension of STEP 3 performed by an Scheme Adminstrator to complete the process with two possible outcomes depending on whether the funds clear:-

- STEP 3 (Funds Clear) - If the funds clear, the State is automatically changed to Active. The Account is still flagged as 'Blocked'. The next time an SA runs 'Blocked Account Report', they will notice that Kristy had attempted to close her Account and that the funds have cleared. The SA can now Cancel her Account. The SA opens the Account and selects the 'Cancel with Letter Option'. This action prints a personalised letter to Kristy as the Account Holder informing her that she has requested to have her account closed. Your final $30 TopUp Voucher is 1234567890. Thank you for using TopItUp and you can rejoin at any time by calling Customer Care on 1300 TOPUPS" and removes Kristy's entitlement of the TopUp Voucher from the allocated $30 pool.

- STEP 3 (Bad Debt or Bad Bank) - If the funds do not clear, TIU will automatically change the State of the Account to Bad Debt or Bad Bank as appropriate. The Account is still flagged as 'Blocked'. The next time an SA runs 'Blocked Account Report', they will notice that Kristy had attempted to close her Account and the funds have not cleared. The SA can now Cancel her Account without providing her a TopUp Voucher as she does not have an entitlement because of the Bad Debt or Bad Bank details. The SA opens the Account and selects the 'Cancel with Letter Option'. This action prints a personalised letter to Kristy as the Account Holder informing her *'that she has requested to have her account closed and that her account is in Bad Debt. Consequently, you are not entitled to a TopUp Voucher. You can ring TopItUp's Financial Department on XXXXXXX to discuss'* and Cancels the Account.

- STEP 5 – George then mails the letter without the TopUp Voucher number to Kristy's address.

Bad Debt or PreRegistered_BadDebt Account is Cancelled

Had the State of Kristy's Account been a Bad Debt or PreRegistered_BadDebt when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

STEP 3 (CCO) - George would have explained to Kristy that her Account does not have an entitlement to a TopUp Voucher as the funds did not clear on the last attempt to draw funds. George says he can close the Account. Kristy agrees. George updates the File Note and uses the 'Cancel as Bad Debt' option. No letter or SMS is printed and TIU Cancels the Account.

Had Kristy complained, George would still take this action and give Kristy the contact handset number for the Financial Administrator to call to discuss.

- STEP 4. George thanks Kristy you for using TopItUp. He does not invite her to rejoin.
- STEP 5. No action as the account is cancelled and no entitlement exists.

Bad Bank or PreRegistered_BadBank Account is Cancelled

Had the State of Kristy's Account been a Bad Bank or PreRegistered_BadBank when she handsetd George, George would have repeated Steps 1 and Step 2 as if the account was Active.

STEP 3 (CCO) - George would have explained to Kristy that her Account does not have an entitlement to a TopUp Voucher as the funds did not clear on the last attempt as the Bank Account details were not correct. George says he can close the Account. Kristy agrees. George updates the File Note and uses the 'Cancel as Bad Bank' option. No letter or SMS is printed and TIU Cancels the Account.

Had Kristy complained, George would still take this action and give Kristy the contact handset number for the Financial Administrator to call to discuss.

- STEP 4. George thanks Kristy you for using TopItUp. He does not invite her to rejoin.
- STEP 5. No action as the account is cancelled and no entitlement exists.

Other Scenarios

Greg's Mobile is Stolen

Greg's mobile (his Dad's actually) is stolen with Greg's Prepaid SIM in the handset at the time. When an SMS is sent using this SIM, TopItUp ascertains Greg's account number from the SIM. Greg handsets

Customer Care using his home handset and speaks to Craig. Craig establishes that Greg is the Account Holder and Greg reports the handset as stolen.

Craig asks Greg for his other contact handset number and verifies the Personal Information on TopItUps database on Greg is accurate.

Craig flags Greg's account as 'Blocked' and records a file note on his account. Blocking an account does not interfere with the processing state of an account. Whatever the processing state was associated with the account prior to the Greg's call is also recorded in the file note. This information is used in any subsequent actions by TopItUp staff to allow consistency to be maintained with the account.

Greg's account is currently Active which means prior to Greg's call, TopItUp would have issed a TopUp Voucher had it been requested. If Greg had received a TopUp Voucher within the past 24 hours, TopItUp would have made a Draw Down on his bank account and TopItUp's logic would continue unaffected updating the processing state of his account regardless of whether the account is flagged Blocked or Unblocked including the rules associated with bad debt processing etc.

Craig explains to Greg that even if someone knows his Password and uses the solen handset in an attempt to request a TopUp Account, that since the handset has been reported stolen, TopItUp will log the SMS request to be investigated for fraud. When an Scheme Administrator reviews the 'potential fraud log files', a decision is made according to TopItUp's current security policy whether to inform the Police. The potential fraud log files contain all details of SMS's sent to TopItUp that are written to the potential fraud log file.

Craig explains that if the handset is found or returned intact, Greg should handset Customer Care and the state of his account will be 'Unblocked' allowing him to use his account normally again.

Until Greg either gets a new SIM or the handset (with SIM) is returned, Greg cannot use his account.

The state of Greg's account was Active when the SIM was reported stolen so Greg is entitled to a TopUp Voucher. Unless the State of Greg's account is 'Bad Debt' or ' PreRegistered_Pending', Greg would eventually be entitled to a TopUp Voucher. Craig asks Greg if he is going to get another Starter Kit and if so, does he want the new SIM to be re-registered with TopItUp in place of the stolen SIM. Greg says 'Yes' and Craig asks Greg to purchase a new Starter Kit from his nearest Network Store and tell the Dealer he is re-registering his account. Craig records Greg's decision on the file note to his account.

Had Greg decided not to register a new SIM, he is entitled to a TopUp Voucher. Had this been the case, Craig would have printed a TopUp voucher and mailed the voucher to Greg's account address (after verifying the address). The voucher is mailed to protect the accountholders right to the TopUp Voucher in the event that this was an attempt by another person to defraud the system. Accompanying the TopUp Voucher

would be a thankyou letter from TopItUp. The Account State would be manually changed by Craig to Cancelled.

Greg Re-Registers his Stolen Account

The state of Greg account remains Blocked until he gets a new Starter Kit (and possibly a new or secondhand handset to replace his Father's stolen handset). He goes to the Dapto Network Communication Store and tells Jock that he wants to buy a Starter Kit and use it to Re-Register a his account. Jock gets Greg to complete a Registration Form and Direct Debit Authority. When completing the Registration Form, Jock gets him to tick the 'Are you Re-Registering an Existing Account' box and Jock asks him to complete the space titled 'Old Handset Number' with the number of his stolen mobile. Jock explains his new account should be registered overnight.

Jock faxes Greg's Registration Form to TopItUp. When Ann goes through the Registration forms the following morning, she notices that Greg's Application is for a Re-Registration. She creates the new account which sets the state of the new account to Pre-Registered. Ann opens up the 'Account Cancellation' screen and picks the 'Cancel an account and transfer Entitlement to a New Account' option. Ann is prompted to enter the account number of the account to be cancelled and enters Greg's old handset number. She notes that the state of this account is 'Active' which means that Greg has an entitlement to a TopUp Voucher.

Ann is prompted to enter the account number of the Pre-Registered Account which she does. TopItUp then asks her to confirm the cancellation of the old account and to change the entitlement. Ann presses the OK button.

The system changes the state of the old account to Cancelled, creates a link to the new account, changes the state of the new account to Active and sends an SMS to Greg's new account welcoming him to TopItUp. Greg could Request a TopUp immediately and TopItUp would send the TopUp Voucher to his new account.

Had the state of Greg's old account been pending when the handset was stolen, it would be unlikely that the state was still pending one day after he had been ins tore for a new Starter Kit, but if had been the case, TopItUp would transfer the state as Pending and not sent the Welcoming SMS until the Draw Down of funds had been cleared. Had the DrawDown resulted in a Bad Debt, the state of the new account would be a Bad Debt.

Greg initially signed up with Network Wollongong. Each TopUp Voucher ordered on his old account resulted in a commission to this store. When Greg re-registered, he did this through Network Dapto. Dapto will not get the commission for the entitlement transferred to the new account, but every TopUp Voucher that is successfully Drawn Down will result in a commission to Jock at Dapto.

James does not live near a Network Store

Greg writes to his brother James at Tennant Creek telling him about TopItUp. Greg knows that James uses Optus Prepaid but has trouble getting TopUp vouchers.

James handsets Greg and asks where he can signup. Greg checks the Hot to Guide and notices that James can get a Registration Form and Direct Debit Authority Network to complete by

- downloading the forms from TopItUps website www.topitup.com.au; or
- ringing Customer Care and requesting the forms be mailed out.

James downloads the forms as 'pdf' files and prints them out. There is no dealer account nominated on the form. The download also includes the 'How to Use Guide' and instructions on how to complete the forms correctly and where to fax or mail them. James completes the forms nominates his prepaid number and signs the T&Cs, and the Direct Deposit form. He mails the forms to TopItUp which starts the Registration process.

Kristy is Concerned about her Privacy

TopItUp will provide Personal Information to Registered Account Holders only.

Kristy saw a special last Sunday night on 60 Minutes regarding the new Privacy obligations on Private Sector organizations.

On Monday morning she gets an SMS from TopItUp telling her about a new range of ringtones that she can get using TopItUp. She remembers that she checked the Send Info box on the Registration Form when she signed up which gives TopItUp permission to send her this SMS.

She did not notice that Lee had TopItUp's Privacy Statement on the sales counter. She checks the 'How to Guide' and reads that she view her Personal Information at a Network Communication Store after mailing, emailing or faxing her request to Jayson Packett, TopItUps Privacy Officer.

She decides to email TopItUp requesting that she views the Peronal Information for both Matt's account and her account at Network Wollongong. When Jayson reads her email, her arranges for Joe to print the Personal Information for both accounts. Joe rings Lee and informs him that Personal Information has been requested by Kristy and that she desires to view this in Lee's store. He asks Lee to stand by his Fax and to ring Kristy to arrange a convenient time for her to view the Personal Information. Joe than faxes both accounts to Lee.

When Kristy comes into store, Lee shows Kristy TopItUps Privacy Statement framed on his sales counter. Kristy is entitled to ask Lee for a copy which she does. Lee provides Kristy with the Personal Information for both accounts. Kristy notices that her street name has been mistyped when Ann originally typed Kristy's details into the TopItUp Registration Database. Kristy is in her rights to have TopItUp keep her information accurate and up to date. She asks Lee to fix the street address. While Kristy is in store, Lee handsets TopItUp

Customer Care centre handing the handset over to Kristy so she can identify herself and the change to her address is updated.

Kristy Wants to Change Matt's Password

Kristy has been concerned that Matt stills wants to know his Password and Kristy is becoming nervous. The Password she created for Matt's account when she registered the account is the cat's name and is very easy to guess. She decides to change it. She rings Customer Care and talks to Crig. After Craig verifies that she is the Account Holder of Matt's account, Craig asks her to provide him with the old password. Craig cannot view the Account Holders Password. To change the Password, he must ask the Account Holder for thei Password, type this in and get a match from TopItiUp.

If he does get a match he will ask Kristy to spell her new password and type the new password in. To ensure this is performed correctly, Craig asks Kristy to spell the Password again as he re-enters it. If both entries for the new Password are the same, the new Password is accepted and the Account Holders account is updated.

If the Account Holder and the User are the same person, TopItUp will send an SMS to account holders handset "Your password has been successfully changed". In this instance, the Account Holder and User are different people, so TopItUp does not send an SMS.

Kristy Forgets the Password

Kristy's forgets the new Password for Matt's handset. She rings Customer Care and talks to George. After George verifies that she is the Account Holder of Matt's account and that she has rung using Matt's handset. George asks her additional questions about recent account activity, such as when did you last Request a TopUp. The additional questions are only asked when someone forgets their Password and require that enough information is provided to George for him to believe that she is not someone who may have stolen Kristy's handset and wallet.

If George is confident she is genuine, George will direct TopItUp to send the Password to Matt's handset as an SMS. George as a Customer Care Officer, does not have sufficient access to obtain Kristy's Password.

The TopUp Voucher Value Changes

The System handles the situation of a TopUp Voucher changing value. Since the Account Holder has an entitlement to a TopUp Voucher, the next time a Recharge Order is received, the TopUp delivered is valued at the old TopUp Voucher value and the new voucher is ordered and payment made at the new TopUp Voucher Value.

Vouchers are supplied GST Free

In accordance with existing recharge vouchers purchased through stores, GTS is not paid by the customer on purchase but is levied and paid by the carrier as the service is used independent of the System.

Hostile Attacks

TopItUp will not allow a user to attempt to use the 'Any Mobile' feature using a web based SMS service such as Optus' Info2You service for security reasons.

Legend:
P – indicates Primary responsibility. For TIU means automatic function.

S – indicates secondary responsibility. For TIU means system is used to perform function

	TopItUp IT Infastructure	SMS - T sent by TIU or - C sent by Customer	Scheme Operator	Scheme Administrator	Financial Administrator	Customer Care Operator	System Administrator	Software Support	Dealer Support	Privacy Officer	TopItUp Website	Dealer	Customer	Customer Bank	Diammond - CBA	CBA Online Banking
Customer Enquiries	S			S		P					P	P	P			
Dealer Enquiries				S					P			P P				
Instore/Web Registration											P web	P store	P			
Deliver Rego Forms												P store	P web			
PreRegister Customer	P		P													
Initial Draw Down including load RBFM	P		P	S										S	P	
Payment & Exception Report			S	P	S											P
Initial Bad Debts	P		P										S			
Customer Activation	P															
Welcome Message	P	T														
Request a TopUp	P	C											P			
SMS TopUp Voucher to Account Handset	P	T											S			
Draw Down including load both R & ABFM	P			P										S	P	
Bad Debt Management	S			P	P											P
Replenish Unallocated Vouchers	S			P	P	S										
Pay Dealer Commissions	S					P									P	S
Bad Attempt – Fraud Investigation	P	C/T		S		S	P									
Cancel an Account	S	T		P		P	P						P			
Privacy Issues	P		S	S	S	P	P	S		P	P	P	S			
Operations Reports	S		S		P											
Financial Reports	S				P		P									
End of Day Processing	S				S		P	S							P	S

The Claims defining the Invention are as follows:

1. A system and method comprising a scheme "scheme" including infrastructure, computer software and components requiring a user "customer" to enrol into the scheme by purchasing an entitlement to a prepaid product or service, which scheme subsequently allows the customer to utilise the entitlement by allowing the customer to have wireless and instant access and delivery of the prepaid product and/or service in accordance with the business rules of the scheme.
2. A system and method as claimed in claim 1, whereby a scheme customer authenticates and authorises the scheme transaction by use of a scheme user name or number and password combination or by other biometric means such as face recognition or by any other means capable of being implemented on a wireless device.
3. A system and method as claimed in claim 1, which requires a customer to authorise the scheme to acquire funds from the customer's financial institution account or facility so as to initiate and maintain the customer's entitlement to a prepaid product or service while ever the customer participates in the scheme.
4. A system and method as claimed in claim 3, wherein the scheme management software initiates a process to interact with the customer's financial institution or facility to acquire appropriate funds to the value equivalent of the enrolment entitlement of the prepaid product and/or service.
5. A system and method as claimed in claim 1, wherein the customer initiates a request using an electronic wireless device to the scheme management infrastructure to acquire the entitlement, which if approved by the scheme, allows the scheme to provide such prepaid products and/or services to be delivered electronically to the same said device or to an alternate customer nominated device.
6. A system and method as claimed in claim 5, wherein once an entitlement has been delivered by the scheme management software to fulfil a customer's request, the scheme management software then initiates a process to interact with the customer's financial institution or facility to acquire additional funds to the equivalent value of the enrolment entitlement or any subsequent changes made by the customer to an alternate or additional prepaid product or service.
7. A system and method as claimed in claim 1, whereby a customer requesting cancellation from the scheme has the right to submit a final request to the scheme for their remaining entitlement according to the business rules of the scheme.
8. A system and method as claimed in claim 1, whereby an agent or agents that are service providers to the scheme and have been authorised to be part of the components that allow a customer to enrol are provided a margin paid and settled by the scheme, based on the value of the prepaid products and services purchased both initially and subsequently by customer's signed up by them using the scheme.
9. A system and method as claimed in claim 1, that allows a customer to purchase a product and /or service on a non-recurring entitlement basis and which are delivered instantly to the customer's wireless device and are subsequently indirectly paid by the customer to the scheme by the scheme

initiating a funds transfer from the customer's financial institution or facility by means of the payment authority provided by the customer in claim 3.

10. A system and method as claimed in claim 9, which allows third parties to provide products and/or services to the scheme, through a scheme provided "content gateway", for resale to customers of the scheme and to be paid a price less a margin on the value of prepaid products and/or services provided which margin is retained by the scheme.

11. A system and method as claimed in claim 1, that allows a scheme authorised third party, using the third parties own system and method "third party scheme", to sell their products and/or services to customers of the scheme by sending a payment request to the scheme by using an authentication link provided by the scheme's infrastructure and components, allowing the third party to be paid a price less a margin for the products and/or services purchased by the customer by way of the scheme's payment facility, if such payment request is approved by the scheme.

12. A system and method as claimed in claim 11, whereby the customer uses the scheme's authentication framework to be identified.

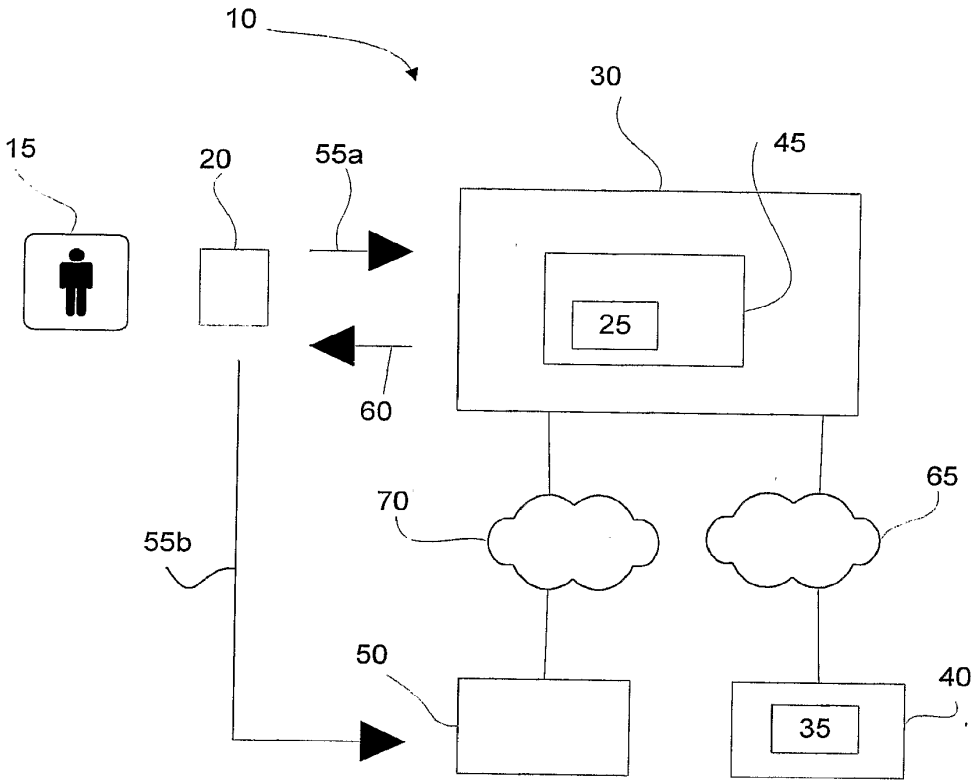
13. A system and method as claimed in claim 11; whereby the customer uses the scheme's payment framework and does not provide any of their financial institution payment or facility details to the third party scheme.

14. A system and method as claimed in claim 13; whereby the scheme allows the customer to purchase or pay for products and/or services at time of request "online" from the scheme authorised third party, if said customer has authorised the scheme to participate in such third party schemes.

15. A system and method as claimed in claim 13; whereby the scheme allows the customer to purchase products and/or services that are subsequently delivered to the customer after the customer payment has settled with the scheme's financial institution "off line" from the scheme authorised third party, if said customer has authorised the scheme to participate in such third party scheme.

16. A system and a method substantially and hereinbefore described with reference to the accompanying drawings.

Figure 1



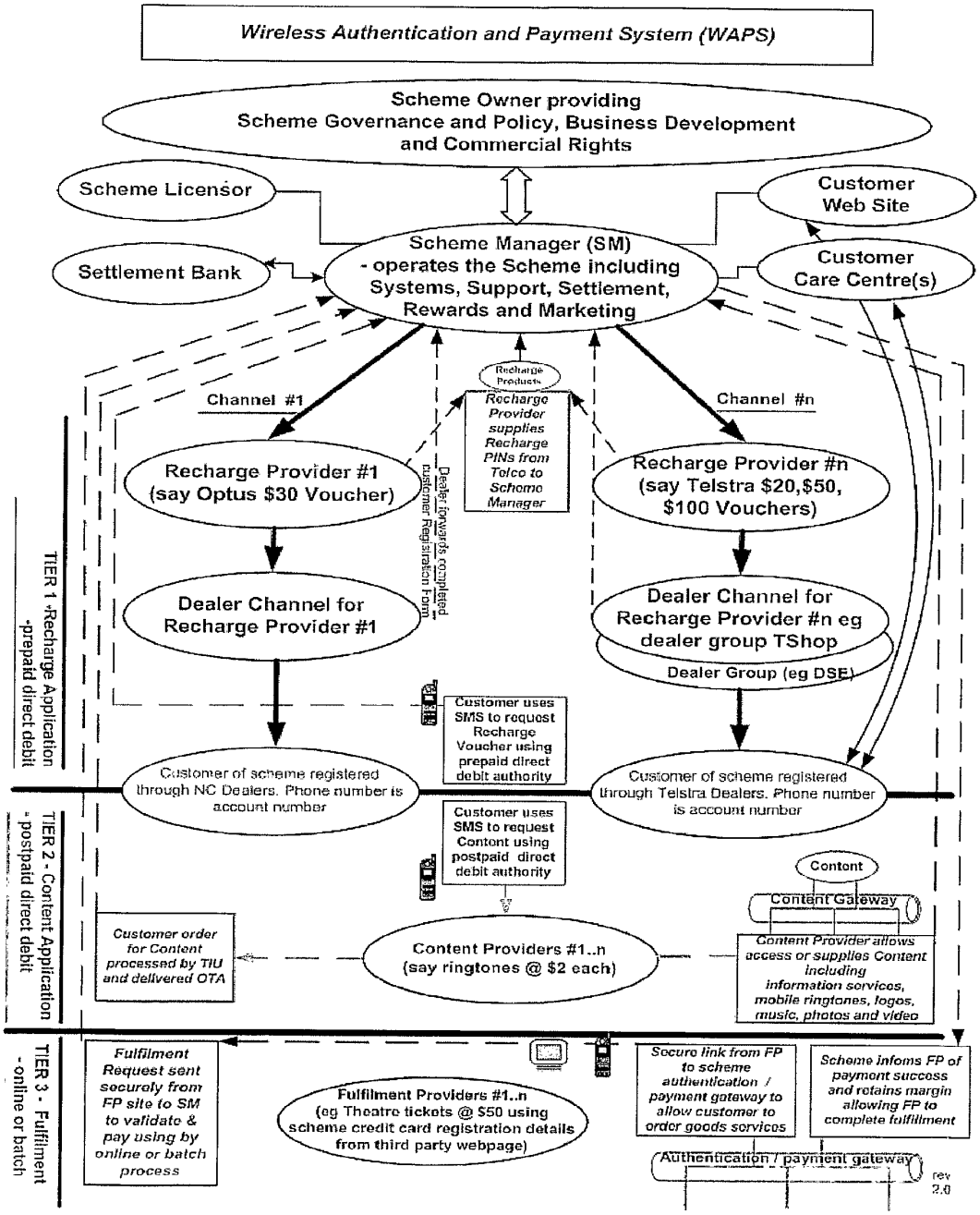


Figure 2

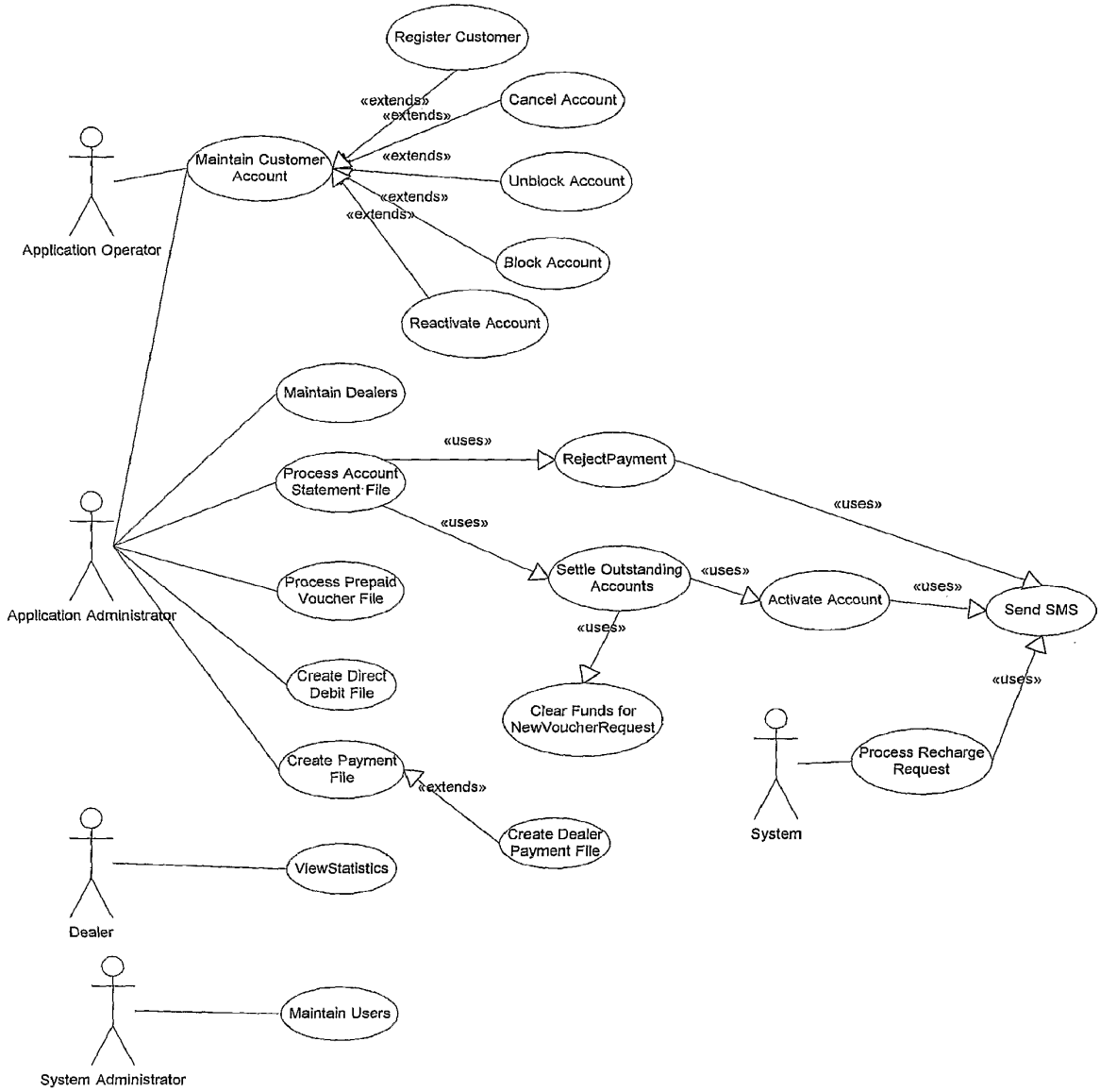


Figure 3

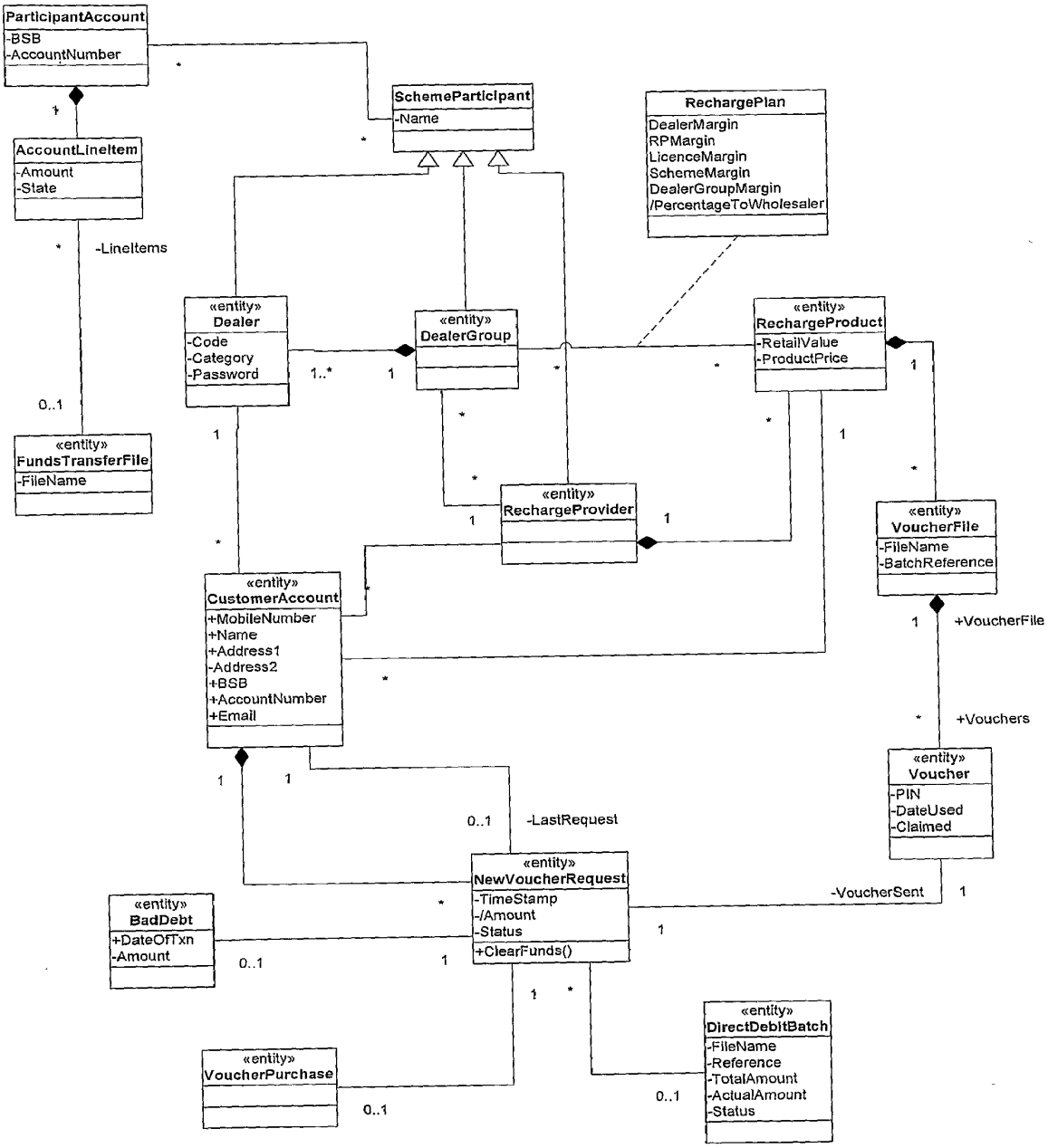

ParticipantAccount
-BSB
-AccountNumber
AccountLineItem
-Amount
-State
-LineItems
FundsTransferFile
-FileName
SchemeParticipant
-Name
RechargePlan
DealerMargin
RPMargin
LicenceMargin
SchemeMargin
DealerGroupMargin
/PercentageToWholesaler
«entity»
Dealer
-Code
-Category
-Password
«entity»
DealerGroup
«entity»
RechargeProduct
-RetailValue
-ProductPrice
«entity»
RechargeProvider
«entity»
VoucherFile
-FileName
-BatchReference
+VoucherFile
+Vouchers
«entity»
CustomerAccount
+MobileNumber
+Name
+Address1
-Address2
+BSB
+AccountNumber
+Email
«entity»
Voucher
-PIN
-DateUsed
-Claimed
-LastRequest
«entity»
NewVoucherRequest
-TimeStamp
-/Amount
-Status
+ClearFunds()
-VoucherSent
«entity»
BadDebt
+DateOfTxn
-Amount
«entity»
VoucherPurchase
«entity»
DirectDebitBatch
-FileName
-Reference
-TotalAmount
-ActualAmount
-Status

Figure-4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/01126

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/60, G06F 153/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI: IPC G06F 17/60, 153/00 and keywords: prepaid, recharg+, voucher?, wireless, mobile?, telecommunication?, payment, paying and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0115424 A (BAGOREN et al.) 22 August 2002 entire document, see in particular paragraphs [0006] to [0010]	1-16
	WO 01/74974 A (SIEMENS AKTIENGESELLSCHAFT) 11 October 2001	
X	abstract	1
Y	abstract	2-7
	US 4706275 A (KAMIL) 10 November 1987	
X	entire document	1
Y	see in particular columns 3 and 4	2-7

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 October 2003	29 OCT 2003
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**CHARLES BERKO** Telephone No : (02) 6283 2169

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/01126

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2002/0065774 A (YOUNG et al.) 30 May 2002	
X	entire document	1
Y	see in particular paragraphs [0007] to [0025]	2-16
	US 6236851 B (FOUGNIES et al.) 22 May 2001	
X	entire document	1
Y	see in particular column 3 line 49 to column 4 line 51	2-16

Form PCT/ISA/210 (continuation of Box C) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/01126

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2002115424	WO	02082797				
WO	0174974	BR	0109641	EP	1269739	US	2003071115
US	4706275						
US	2002065774	AU	20491/01	EP	1014646	EP	1107198
		JP	2001243386	US	2002123965	WO	0141419
		WO	02069085				
US	6236851	US	5722067	US	5854975	US	6157823
		US	2001021648				

END OF ANNEX

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number
WO 2004/053640 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/038692

(22) International Filing Date: 5 December 2003 (05.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/431,567 6 December 2002 (06.12.2002) US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

(71) Applicants and
(72) Inventors: **GOLDHWAITE, Scott** [US/US]; 15 Oregon court, Hingham, MA 02043 (US). **GRAYLIN, William** [US/US]; 229 Washington Street, Woburn, MA 01801 (US).

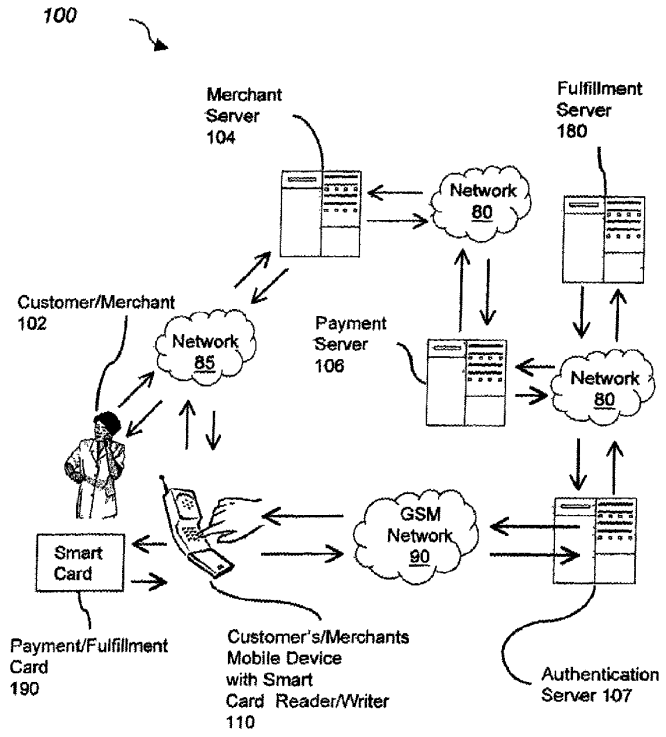
(74) Agent: **COLLINS, Aliki, K., PH., D.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILMENT DIGITAL GOODS



(57) Abstract: An electronic payment and fulfillment system utilized by a customer for purchasing a digital good includes a merchant server 104, a payment server 106, an authentication server 107, a fulfillment server 180 and a communication device 110. The communication device 110 includes a payment card module and the payment card module receives a payment card 190 and reads payment card identification information stored in the payment card. The communication device 110 transmits the payment card identification information to the payment server 106 and then receives the digital good from the fulfillment server 180 and stores it onto the payment card 190. Communications from and to the communication device 110 pass through the authentication server 107.

WO 2004/053640 A2

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILLMENT OF DIGITAL GOODS

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/431,567 filed on December 6, 2002 and entitled SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILLMENT OF DIGITAL GOODS which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, and 10/695,585, filed on July 26, 2002, July 23, 2003, and October 28, 2003, and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", and "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for mobile payment and fulfillment of digital goods, and more particularly to a mobile payment transaction and fulfillment of digital goods with a strong authentication.

Background of the Invention

Smart Cards used in the financial services industry are rapidly replacing magnetic stripe cards. The primary reason for the migration to smart cards is the increased level of security that smart cards can provide. Smart Cards have an embedded Integrated Circuit (IC) that enables a highly secure computing environment to store sensitive information, such as credit card information, medical information, digital certificates and biometric data. Smart Cards are also used as a secure repository for "digital goods", such as electronic cash (e-Cash), electronic tickets (e-Tickets), electronic coupons (e-Coupons), loyalty points (i.e. frequent flyer miles, frequent shopper points), credits for pre-paid mobile airtime, credits for pre-paid utilities, and

digital rights management (DRM) certificates for accessing multi-media applications. The greatest use of these "e-Purses" on smart cards are e-Cash schemes from Visa International and MONDEX International and transit token systems that comply to the MIFARE (Philips) and Octopus (Sony). While the use of smart cards has been the catalyst for e-Purse business, the challenge is the expense in installing and maintaining the card reader/writer infrastructure required to enable users to "top up" or "reload" or "download" digital goods and monetary value to their smart cards. Typically, users can load/reload digital goods and value onto the card by using an Automated Teller Machine (ATM), a kiosk or a Point of Sale (POS) system in a store to transfer money from a checking account, savings account, a credit card account or by inserting cash into the ATM. These ATMs are typically located at the entrance to the transit stations, small merchant stores and bank outlets. The number and availability of the smart card reader/writer equipment determine the amount of usage of smart cards. There is a need for a secure, low cost system that can be used to fulfill and pay for digital goods.

Summary of the Invention

This invention features an electronic payment and digital good fulfillment system utilized by a customer to pay for the purchase of a good and/or a service with a physical or virtual payment instrument. The present invention provides consumers or merchants with the ability to download digital goods such as electronic cash (e-Cash), electronic coupons (e-Coupon), electronic tickets (e-Ticket), electronic transit tokens, credits for pre-paid mobile airtime, credits for pre-paid utilities, credits for other types of pre-paid accounts, a digital receipt or ticket that can be utilized at a later point to further receive digital goods (i.e., a Hidden Rechargeable Number "HRN" for pre-paid top up), digital rights management (DRM) certificates and digital media such as music, software, movies, books and other digital content to a smart card, contactless smart card or magnetic stripe card.

In general, in one aspect of this invention features an electronic payment and fulfillment system utilized by a customer for purchasing a digital good including a merchant server, a payment server, an authentication server, a communication device, and a fulfillment server. The merchant server is programmed to receive a purchase order from the customer for the purchase of the digital good, and to create a digital

order comprising purchase order information. The payment server is programmed to receive the digital order from the merchant server and to further route the digital order. The authentication server is programmed to receive the digital order from the payment server, format the digital order into a first message and further route the first message. The communication device includes a payment card module and the payment card module is adapted to receive a payment card and read payment card identification information stored in the payment card. The communication device is also adapted to receive the first message from the authentication server, display the first message to the customer, request and receive authorization for payment for the purchase order with the payment card from the customer, retrieve the payment card identification information, request and receive payment card security information from the customer, and route the authorization and the payment card identification and security information to the authentication server. The authentication server further routes the authorization and payment card identification and security information to the payment server and from the payment server to a financial institution. The financial institution is asked to execute the payment and to send a payment confirmation through the payment server to the merchant server and to the authentication server. The fulfillment server is programmed to receive the payment confirmation from the payment server and transmit the digital good via the authentication server to the communication device. The communication device then stores the digital good onto the payment card.

Implementations of this aspect of the invention include the following. The communication device may be a wireless communication device or a wired communication device. The merchant server, the payment server, the authentication server, the fulfillment server and the communication device are adapted to send and receive messages among each other via a first network and the wireless communication device is adapted to send and receive messages to the authentication server via a second network and the second network may be a wireless network. The wireless communication device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof or combinations thereof. The wireless network may be a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) or a private communication network The wireless wide

area network (WWAN) may be a Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The wired communication device may be a telephone and the first network may be a telecommunications network. The wired communication device may be a computer and the first network may be the Internet. The payment card may be a smart card such as a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card or combinations thereof. The payment card may be a magnetic stripe card. The merchant server may receive the purchase order from the customer via the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), or face-to-face communication with the customer. The wireless communication device may have a subscriber identification module (SIM) card slot and the payment card module may be electrically connected to the SIM card slot. The payment card information may be cardholder identification information, card identification information, authentication information, card issuer information, or financial institution information. The digital good may be electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements (DRM) certificates, electronic transit tokens, music, software, movies, or books. The merchant server and the fulfillment server may be one entity. The customer may place the purchase order to the merchant server via the communication device. The communication device may further include a shopping application and the customer may utilize the shopping application, to select the digital good, to place the purchase order, to authorize, authenticate and pay with the payment card, and to store the digital good onto the payment card. The payment card module may include a payment card reader and writer module. The communication device may further include a digital good generation application and the digital good generation application may receive a digital receipt for the digital good and generate the digital good. The first message may have a format such as Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats.

In general in another aspect the invention features an electronic payment and fulfillment method utilized by a customer for purchasing a digital good including placing a purchase order with a merchant server for the digital good and choosing to pay via a communication device. Next, providing the merchant server with identification information for the communication device and creating a digital order comprising purchase order information and the identification number for the communication device by the merchant server. Next, routing the digital order to a payment server and from the payment server to an authentication server. Next, formatting the digital order into a first message by the authentication server and routing the first message to the communication device. Next, displaying the first message on the communication device and requesting and receiving authorization of payment from the customer. Next, retrieving identification information of a payment card from the communication device and requesting and receiving security information of the payment card from the customer via the communication device. Next, routing the authorization and the payment card identification and security information through the authentication server to the payment server and from the payment server to a financial institution. Next, executing the payment at the financial institution and sending a payment confirmation to the payment server. Next, routing the payment confirmation from the payment server to the merchant server and to a fulfillment server and transmitting the digital good from the fulfillment server via the authentication server to the communication device. Finally, storing the digital good onto the payment card by the communication device.

Among the advantages of this invention may be one or more of the following. Combining a smart card reader (contact or contactless) with a mobile phone can dramatically increase the number of smart card reader points of sales in the marketplace to create more convenience for consumers and more opportunities for merchants. Consumers or merchants with a mobile phone equipped with a smart card reader would be able to load value to their cards (contact or contactless) anytime, anywhere. Using a secure, non-repudiatable payment enables the secure over-the-air download of digital goods. In countries or locations where a "land-line" telephone connection required by an Automated Teller Machine (ATM) or merchant Point of

Sale (POS) system is either too expensive or not feasible, a mobile device equipped with a smart card reader is significantly more cost effective and convenient.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of a system for digital goods purchase and fulfillment using a mobile device with a smart card reader according to this invention.

FIG. 2 illustrates prior art circuitry for the mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone.

FIG. 3 illustrates circuitry for a mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with a contactless smart card reader/writer.

FIG. 4 is a diagram of a payment and digital goods fulfillment system according to this invention.

FIG. 4A is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 4B is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 4C is a diagram of another embodiment of a payment and digital goods fulfillment system according to this invention.

FIG. 5 illustrates circuitry for a mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with a magnetic stripe card reader/writer.

FIG. 6 is a flow diagram for a shopping application on a mobile device.

FIGS. 6A – 6L illustrate an example user scenario for mobile payment and digital goods fulfillment.

Detailed Description of the Invention

The present invention provides a smart card payment and digital goods fulfillment system. The smart card has the ability to retain stored value or other types of information within the card. These "digital goods" are electronic, virtual information that represents value such as electronic cash (e-Cash), electronic coupons (e-Coupon), electronic tickets (e-Ticket), electronic transit tokens, credits for pre-paid mobile airtime, credits for pre-paid utilities, credits for other types of pre-paid accounts, a digital receipt or ticket that can be utilized at a later point to further receive digital goods (i.e., a Hidden Rechargeable Number "HRN" for pre-paid top up), digital rights management (DRM) certificates and digital media such as music, software, movies, books and other digital content. The payment transaction and digital goods fulfillment system allows the purchase of digital goods and reception and storage of the digital goods on a smart card.

Referring to FIG. 1 and FIG 4, a payment transaction and digital goods fulfillment system 100 includes a customer 102 with a smart card 190 and a mobile phone device 110 equipped with a smart card reader/writer, a merchant server 104, a payment server 106, an authentication system 108, a financial institution 112 and a fulfillment server 180. The authentication system 108 includes an authentication server 107 that is adapted to send and receive messages in a short message service (SMS) format to the mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive the payment card 190 or has a built-in payment card (not shown). After having placed an order for digital goods via the Internet, Short Message Service (SMS), Wireless Application protocol (WAP), or voice 85, customer 102 is asked to choose a payment method. The customer 102 chooses to pay via her mobile phone 110 and gives her mobile phone identification information to the merchant server 104 (114). In one example, the mobile phone identification information is the mobile phone number. The merchant server 104 routes the customer's mobile phone number and information about the purchase order to the payment server 106 (116). The payment server 106 contacts the authentication server 107 and routes the customer's mobile phone number and information about the purchase (118). The authentication

server 107 sends an SMS message to the customer's mobile phone 110 through an SMS carrier 109 (120). The customer 102 receives the SMS message asking her to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, uses the smart card 190 that is associated with her mobile phone 110 (188) and enters a security code associated with the smart card to pay and authenticate her purchase (124). In one example, the security code is a personal identification number (PIN). Other examples include a password, digital signature, and a biometric identifier, i.e., retina scan, fingerprint, DNA scan, voice characteristics. The payment card 190 is identified with information that is embedded in the card. In one example the identification information is a payment card number. Other examples of payment card identification include an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card, expiration date of the payment card, and a digital signature. The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107. The SMS message includes the authorization result and payment transaction information (126). The authentication server 107 routes the authorized purchase order and authenticated card to the payment server 106 (128). The payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the purchase order information (130). The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134), presents a digital receipt to the fulfillment server 180(181) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card. Finally, the digital goods are transferred from the mobile phone 110 to the smart card 190 (189).

The message routing 114 occurs over communication network 85, message routing 116, 134, occurs over communication network 82, message routing 118, 128, 136 occurs over communication network 86, message routing 120, 122, 124, 126, 138, occurs over communication network 90, and message routing 130, 132, occurs over communication network 84. Communication between the authentication server 107 and the SMS carrier 109 occurs over network 88, and communication between the fulfillment server 180 and the authentication server 107 is over network 80. In one example, communication networks 80, 82, 84, 85, 86, and 88 are the Internet and communication network 90 is a wireless network. In another example communication network 85 is wireless or wire line, voice or data network. The wireless network 85 and 90 may be a Wireless Wide Area Network (WWAN) (i.e., GSM, TDMA, CDMA, 3G, iDEN, Mobitex, and DataTac), a Wireless Local Area Network (WLAN) (i.e., 802.11a, 802.11b), or a Personal Area Network (PAN) (i.e., Bluetooth, Infrared). Other examples of communication networks 80, 82, 84, 85, 86, 88 and 90 include private voice and data networks, and public voice and data networks. Message routing 114-140 is encrypted.

In the embodiments of FIG. 1 and FIG.4, the fulfillment server 180 and the merchant server 104 are two separate entities. For example, the merchant server 104 contains the merchant catalog of music or documents that can be downloaded and the fulfillment server 180 is the storage repository for the actual digital media. In another embodiment the fulfillment server 180 and the merchant server 104 are the same entity (not shown).

In the embodiment of FIG. 4A an order is initiated directly from the mobile phone device. The customer 102 interacts with a shopping application 600 on the mobile phone device 110 (shown in FIG. 6 and FIGS. 6A – 6L) to initiate, place, authorize and fulfill an order.

Referring to FIG. 4A, the system for placing an order directly from the mobile phone device includes a customer 102 with a smart card 190 and a mobile phone device 110 equipped with smart card reader/writer, a merchant server 104, a payment server 106, an authentication system 108, a financial institution 112 and a fulfillment server 180. The authentication system 108 includes an authentication server 107 that is adapted to

send and receive messages in a short message service (SMS) format to mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive the payment card 190 or has a built-in payment card (not shown). The customer 102 makes the purchase selection on the mobile device using a shopping application 600 and is prompted to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, uses a smart card 190 that is associated with her mobile phone 110 (188) and enters a security code associated with the smart card to pay and authenticate her purchase (124). The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107(126). The SMS message includes the order details, merchant information, authorization result, and payment transaction information. The authentication server 107 routes the authorized purchase order and authenticated card to the payment server 106 (128). The payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the order information (130). The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134), presents a digital receipt to the fulfillment server 180 (181) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card and the digital goods are transferred to the smart card 190 (189).

In one example the mobile phone device 110 is a programmable device, such as a Personal Digital Assistance (PDA)-type phone and the shopping application 600 is a series of menus on the mobile phone device that guide the customer through the shopping process. In another example, the mobile phone device 110 is a non-programmable phone and the shopping application 600 is an application that is

installed on the mobile phone and accessed via the phone's interface. Referring to FIG. 6 and FIG. 6A to FIG. 6L, the shopping application 600 includes the following operations. The customer 102 selects a transit ticket purchase application on her PDA-type phone (602). Next, the customer 102 selects the desired fare amount (604). Alternatively, the customer 102 selects the origin station (605), the destination station (606), the fare type (607), and the fare is calculated by the application (608). Next, the customer 102 initiates the payment transaction and inserts a payment card (610). Next, the customer 102 selects the payment instrument on the card (i.e., VISA, Master Card, Amex) (612), and authenticates the payment transaction with her PIN number (614). If her PIN number is valid (616) the transaction is transmitted to the authentication server 107 and processed by the payment server 106, merchant server 104, financial institution 112, and fulfillment server 180 (618). When the payment is confirmed and the desired fare amount is ready to be transferred to the transit card, the application 600 prompts the customer 102 to insert her transit card in the phone card reader (620). Finally, the desired fare amount is transferred to the transit card (622) and the transaction is completed (624).

Referring to FIG. 4B, in another embodiment, the authentication server 107 presents the digital receipt to the fulfillment server. Following the payment authorization from the financial institution 112 a confirmation of the payment transaction is transmitted to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138) and then presents a digital receipt to the fulfillment server 180 (181). The fulfillment server 180 fulfills the customer's order for digital goods by sending the electronic information that represents the digital goods to the authentication server 107 (140). The authentication server 107 transfers the digital goods and sends an SMS message to the customer's mobile phone 110 through the SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the smart card and the digital goods are transferred to the smart card 190 (189).

Referring to FIG. 4C, in another embodiment, the mobile phone device receives a digital receipt that is then transmitted to the smart card, and is then utilized by an application on the smart card such as a transit token or e-Cash application as the authorization to generate digital goods. Following the payment authorization from the financial institution 112 a confirmation of the payment transaction is transmitted to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends a digital receipt 110 and an SMS message confirming the payment transaction to the customer's mobile phone (138). The mobile phone 110 receives the confirmation message and the digital receipt for digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available. An application on the smart card or on the mobile phone generates the digital goods based on the information contained within the digital receipt. The digital goods are created and transferred to the smart card 190 (189).

In another embodiment, the payment authentication instrument may be contained on one or many Subscriber Identity Module (SIM) smart cards for GSM wireless networks or Universal Subscriber Identity Module (USIM) smart cards for 3G wireless networks within the mobile phone 110, or within full-size smart cards inserted into a smart card reader 153 that is either attached to or embedded in the mobile phone device 110 or contained on a contactless smart card that can be accessed by a mobile phone device 110 with a contactless reader. The general concept of connecting additional smart card readers by implementing a connection to the existing SIM connector on a mobile phone is defined in the prior art "Communication Method and Apparatus Improvements" (PCT International Publication Number WO 99/66752), the entire content of which is incorporated herein by reference. This prior art defines the implementation of a mobile phone device attachment 200 that utilizes a Central Processor Unit to coordinate the activities of multiple SIM cards and full-size smart cards (See FIG. 2). The prior art defines the basic design of a mobile phone that provides a smart card reader either attached to the phone as an accessory or embedded into the design of the phone. Co-pending patent application entitled "Mobile Device Equipped with a Contactless Smart Card Reader", the entire content of which is incorporated herein by reference, describes a mobile phone that provides a

"contactless" smart card reader 300 to read/write data to a contactless smart card (see FIG. 3).

In another embodiment, the receiver of the digital goods can be one or many Subscriber Identity Module (SIM) smart cards for GSM wireless networks or Universal Subscriber Identity Module (USIM) smart cards for 3G wireless networks within the mobile phone 110, or a full-size smart cards inserted into a smart card reader that is either attached to or embedded in the mobile phone device 110 or a contactless smart card that can be accessed by a mobile device 110 with a contactless reader or the mobile phone itself.

In another embodiment, the payment authentication card can be a magnetic stripe payment card that is accessed by the mobile phone device utilizing the magnetic stripe card reader 500 described in a co-pending patent application entitled "Mobile Communication Device Equipped with a Magnetic Stripe Reader", the entire content of which is incorporated herein by reference, (see FIG 5).

Other embodiments are within the scope of the following claims. For example, the smart card reader and/or payment card reader is adapted to connect to the mobile phone device through the mobile phone device's accessory connection point such as serial, USB, Compact Flash, Infrared, Bluetooth and Secure Digital. The digital goods may be fulfilled to a dual-interface contact/contactless smart card, or to a multi application "combi" contact/contactless smart card. The authentication of the customers Personal Identification Number (PIN) may be processed online at the financial institution or with a third-party server-side wallet account. The payment instrument may an account established with a server-side wallet. A browser on the mobile device may be utilized for entering the payment information. The payment information may be verbally transcribed to a customer service representative or a speech recognition system. The payment information may also be transcribed utilizing an Interactive Voice Response system. The digital goods are transferred to a customer's virtual or server-side account. The digital goods that are downloaded may be a digital receipt for goods to be fulfilled at a later time by the customer such as the online generation of a Hidden Rechargeable Number (HRN) for pre-paid top up that the customer will utilize to top up a pre-paid mobile, utility or other type of pre-paid

account. The mobile device may be held by a merchant to accept payment from and fulfill digital goods to a plurality of customers. In addition to SMS messaging via the SMS Carrier 109 between the authentication server 107 and the mobile phone 110, the communication between the authentication server 107 and the mobile phone 110 may be via a proprietary message protocol that utilizes User Datagram Protocol (UDP) on top of Internet Protocol (IP). This proprietary message protocol is adapted to be used with wireless networks that support Transmission Control Protocol/Internet Protocol (TCP/IP). These wireless networks include Bluetooth, 3G, GPRS, 2.5G, Infrared, WCDMA, CDMA200, 802.11a and 802.11b. The mobile phone identification information may be an Internet Protocol (IP) address. The communication networks 80, 82, 84, 86, 88 and 90 may be wireless or wired networks. The communication networks 80, 82, 84, 86, 88 and 90 may be non face-to-face via the Internet, VPN (Virtual Private Network), cable network, data network, telephone network, private voice and data networks, public voice and data networks, and mail or person to person. Payment card identification may occur via the payment card number or via an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card. The authentication server may also utilize a password, digital signature, or a biometric identifier, i.e., retina scan, fingerprint, voice characteristics, to authenticate the payment transaction. The payment authentication instrument may be contained in the contactless smart card, on the SIM smart cards within the mobile phone 110, or within another full-size smart card that needs to be inserted into a smart card reader slot. The communication mobile phone device may be a mobile wireless device and the second network may be a wireless network. The mobile wireless device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, or combinations thereof. The second network may be a wireless wide area network (WWAN), a wireless local area network (WLAN) or a wireless personal area network (PAN). The communication device may also be a wired communication device and the second network may be a wired network. The wired communication device may be a telephone or a computer and the wired network may be a telecommunications network or the Internet, respectively. The first network may be the Internet or a telecommunication network.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

1. An electronic payment and fulfillment system utilized by a customer for purchasing a digital good comprising:

a merchant server adapted to receive a purchase order from said customer for the purchase of said digital good, and to create a digital order comprising purchase order information;

a payment server adapted to receive said digital order from said merchant server and to further route said digital order;

an authentication server adapted to receive said digital order from said payment server, format said digital order into a first message and further route said first message;

a communication device comprising a payment card module wherein said payment card module is adapted to receive a payment card and read payment card identification information stored in said payment card, and wherein said communication device is adapted to receive said first message from said authentication server, display said first message to said customer, request and receive authorization for payment for said purchase order with said payment card from said customer, retrieve said payment card identification information, request and receive payment card security information from said customer, and route said authorization and said payment card identification and security information to the authentication server, and wherein said authentication server further routes said authorization and payment card identification and security information to said payment server and from said payment server to a financial institution, wherein said financial institution is asked to execute said payment and to send a payment confirmation through said payment server to said merchant server and to said authentication server; and

a fulfillment server adapted to receive said payment confirmation from said payment server and transmit said digital good via said authentication server to said communication device, wherein said communication device stores said digital good onto said payment card.

2. The system of claim 1 wherein said communication device comprises a wireless communication device.

3. The system of claim 1 wherein said communication device comprises a wired communication device.

4. The system of claim 3 wherein said merchant server, said payment server, said authentication server, said fulfillment server and said communication device are adapted to send and receive messages among each other via a first network.

5. The system of claim 2 wherein said merchant server, said payment server, said authentication server, and said fulfillment server are adapted to send and receive messages among each other via a first network and said wireless communication device is adapted to send and receive messages to said authentication server via a second network and wherein said second network comprises a wireless network.

6. The system of claim 2 wherein said wireless communication device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof and combinations thereof.

7. The system of claim 5 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

8. The system of claim 7 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

9. The system of claim 4 wherein said wired communication device comprises a telephone and said first network comprises a telecommunications network.

10. The system of claim 4 wherein said wired communication device comprises a computer and said first network comprises the Internet.

11. The system of claim 1 wherein said payment card comprises a smart card selected from a group consisting of a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a

coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

12. The system of claim 1 wherein said payment card comprises a magnetic stripe card.

13. The system of claim 1 wherein said merchant server receives said purchase order by said customer via a route selected from a group consisting of the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), and face-to-face communication with the customer.

14. The system of claim 2 wherein said wireless communication device comprises a subscriber identification module (SIM) card slot and said payment card module is electrically connected to said SIM card slot.

15. The system of claim 1 wherein said payment card information is selected from a group consisting of cardholder identification information, card identification information, authentication information, card issuer information, and financial institution information.

16. The system of claim 1 wherein said digital good is selected from a group consisting of electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements(DRM) certificates, electronic transit tokens, music, software, movies, and books.

17. The system of claim 1 wherein said merchant server and said fulfillment server comprise one entity.

18. The system of claim 1 wherein said customer places said purchase order to said merchant server via said communication device.

19. The system of claim 1 wherein said communication device further comprises a shopping application and wherein said customer utilizes said shopping application, to select said digital good, to place said purchase order, to authorize, authenticate and pay with said payment card, and to store said digital good onto said payment card.

20. The system of claim 1 wherein said payment card module comprises a payment card reader and writer module.

21. The system of claim 1 wherein said communication device further comprises a digital good generation application and wherein said digital good generation application receives a digital receipt for said digital good and generates said digital good.

22. The system of claim 1 wherein said first message comprises a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

23. An electronic payment and fulfillment method utilized by a customer for purchasing a digital good comprising:

placing a purchase order with a merchant server for said digital good and choosing to pay via a communication device;

providing said merchant server with identification information for said communication device;

creating a digital order comprising purchase order information and said identification number for said communication device by said merchant server;

routing said digital order to a payment server and from said payment server to an authentication server;

formatting said digital order into a first message by said authentication server and routing said first message to said communication device;

displaying said first message on said communication device and requesting and receiving authorization of payment from the customer;

retrieving identification information of a payment card from said communication device;

requesting and receiving security information of said payment card from said customer via said communication device;

routing said authorization and said payment card identification and security information through said authentication server to said payment server and from said payment server to a financial institution;

executing said payment at said financial institution and sending a payment confirmation to said payment server;

routing said payment confirmation from said payment server to said merchant server and to a fulfillment server;

transmitting said digital good from said fulfillment server via said authentication server to said communication device; and

storing said digital good onto said payment card by said communication device.

24. The method of claim 23 wherein said communication device comprises a payment card module adapted to receive said payment card and read said payment card identification information stored in said payment card and to receive a digital good and store said digital good onto said payment card.

25. The method of claim 23 wherein said communication device comprises a wireless communication device.

26. The method of claim 23 wherein said communication device comprises a wired communication device.

27. The method of claim 26 wherein said merchant server, said payment server, said authentication server, said fulfillment server and said communication device are adapted to send and receive messages among each other via a first network.

28. The method of claim 25 wherein said merchant server, said payment server, said authentication server, and said fulfillment server are adapted to send and receive messages among each other via a first network and said wireless communication

device is adapted to send and receive messages to said authentication server via a second network and wherein said second network comprises a wireless network.

29. The method of claim 25 wherein said wireless communication device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, programmable versions thereof and combinations thereof.

30. The method of claim 28 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

31. The method of claim 30 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

32. The method of claim 26 wherein said wired device comprises a telephone and said first network comprises a telecommunications network.

33. The method of claim 26 wherein said wired device comprises a computer and said first network comprises the Internet.

34. The method of claim 23 wherein said payment card comprises a smart card selected from a group consisting of a full size smart card, a contactless smart card, a SIM smart card, a USIM smart card, a credit card, a debit card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

35. The method of claim 23 wherein said payment card comprises a magnetic stripe card.

36. The method of claim 23 wherein said placing a purchase order comprises placing a purchase order via a route selected from a group consisting of the Internet, telephone connection, mail order form, fax, e-mail, voice recognition system, shot message service, interactive voice recording (IVR), and face-to-face communication with the customer.

37. The method of claim 24 wherein said communication device comprises a subscriber identification module (SIM) card slot and said payment card module is electrically connected to said SIM card slot.

38. The method of claim 23 wherein said payment card information is selected from a group consisting of cardholder identification information, card identification information, authentication information, card issuer information, and financial institution information.

39. The method of claim 23 wherein said digital good is selected from a group consisting of electronic cash, electronic tickets, electronic coupons, loyalty points, credits for pre-paid mobile airtime, credits for pre-paid utilities, electronic gift certificates, digital rights managements(DRM) certificates, electronic transit tokens, music, software, movies, and books.

40. The method of claim 23 wherein said merchant server and said fulfillment server comprise one entity.

41. The method of claim 23 wherein said customer places said purchase order to said merchant server via said communication device.

42. The method of claim 23 wherein said communication device further comprises a shopping application and wherein said customer utilizes said shopping application, to select said digital good, to place said purchase order, to authorize, authenticate and pay with said payment card, and to store said digital good onto said payment card.

43. The method of claim 24 wherein said payment card module comprises a payment card reader and writer module.

44. The method of claim 23 wherein said communication device further comprises a digital good generation application and wherein said digital good generation application receives a digital receipt for said digital good and generates said digital good.

45. The method of claim 23 wherein said first message comprises a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

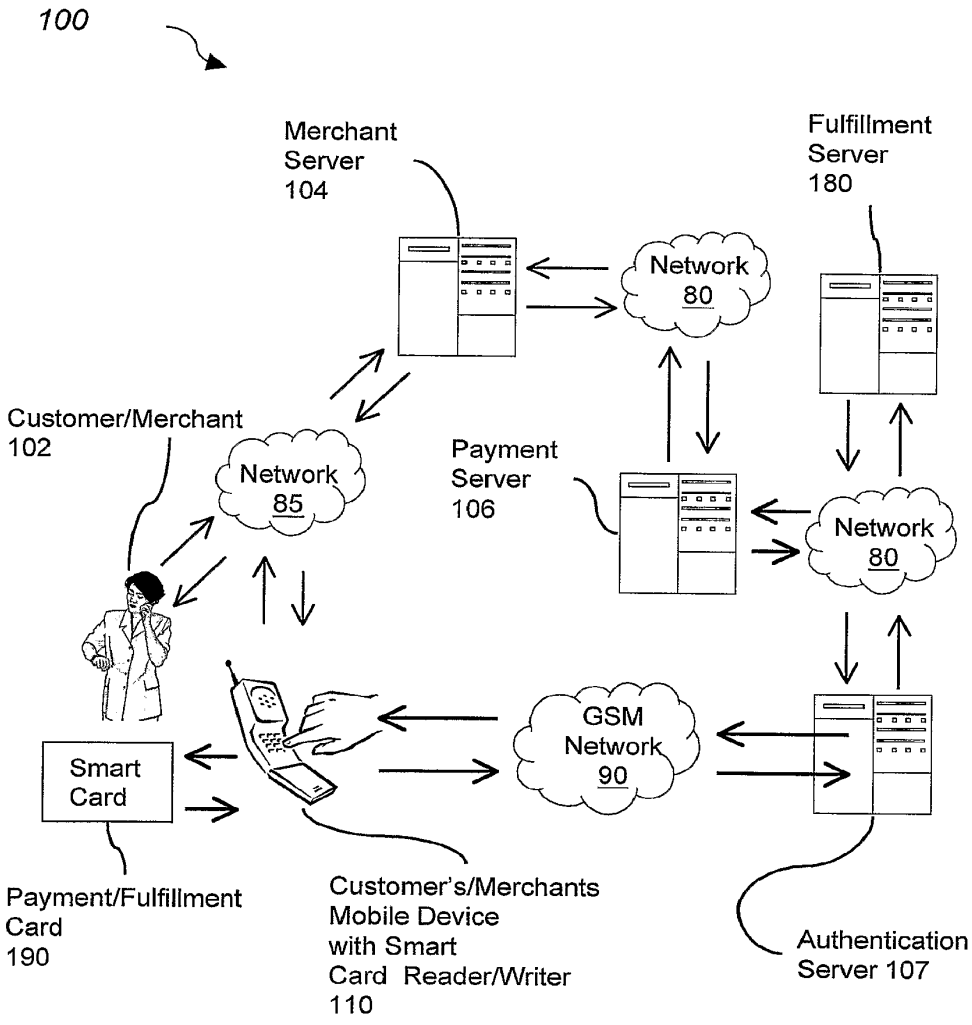

100
Merchant Server 104
Fulfillment Server 180
Network 80
Customer/Merchant 102
Network 85
Payment Server 106
Network 80
GSM Network 90
Smart Card
Payment/Fulfillment Card 190
Customer's/Merchants Mobile Device with Smart Card Reader/Writer 110
Authentication Server 107

FIG. 1

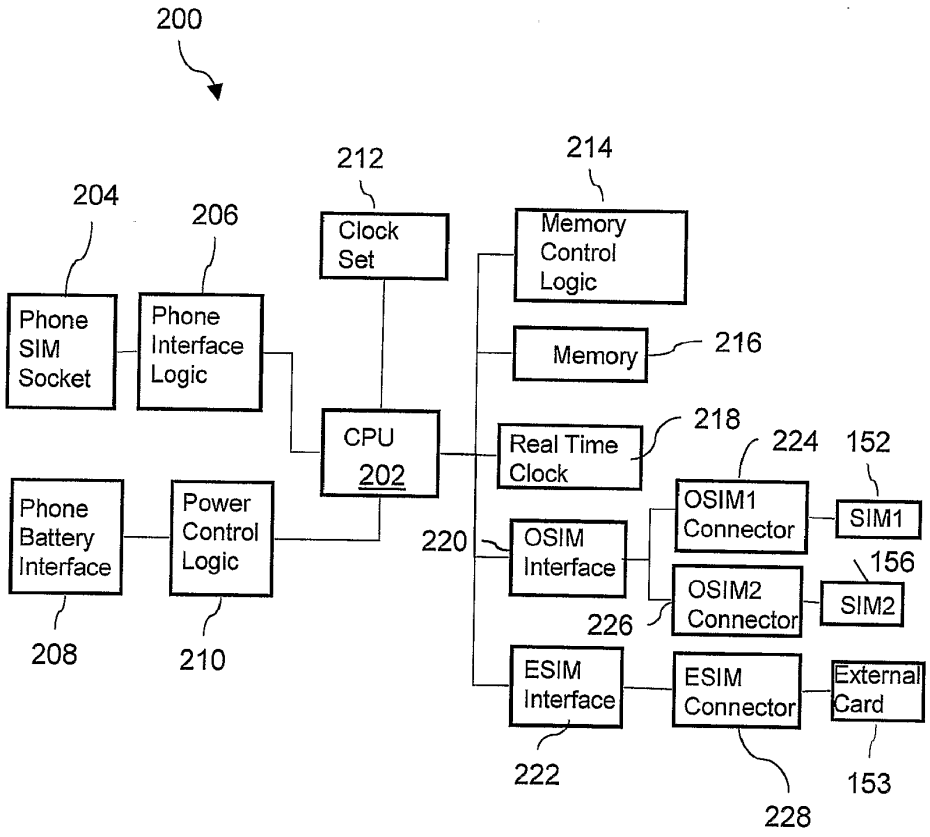


FIG. 2
(Prior Art)

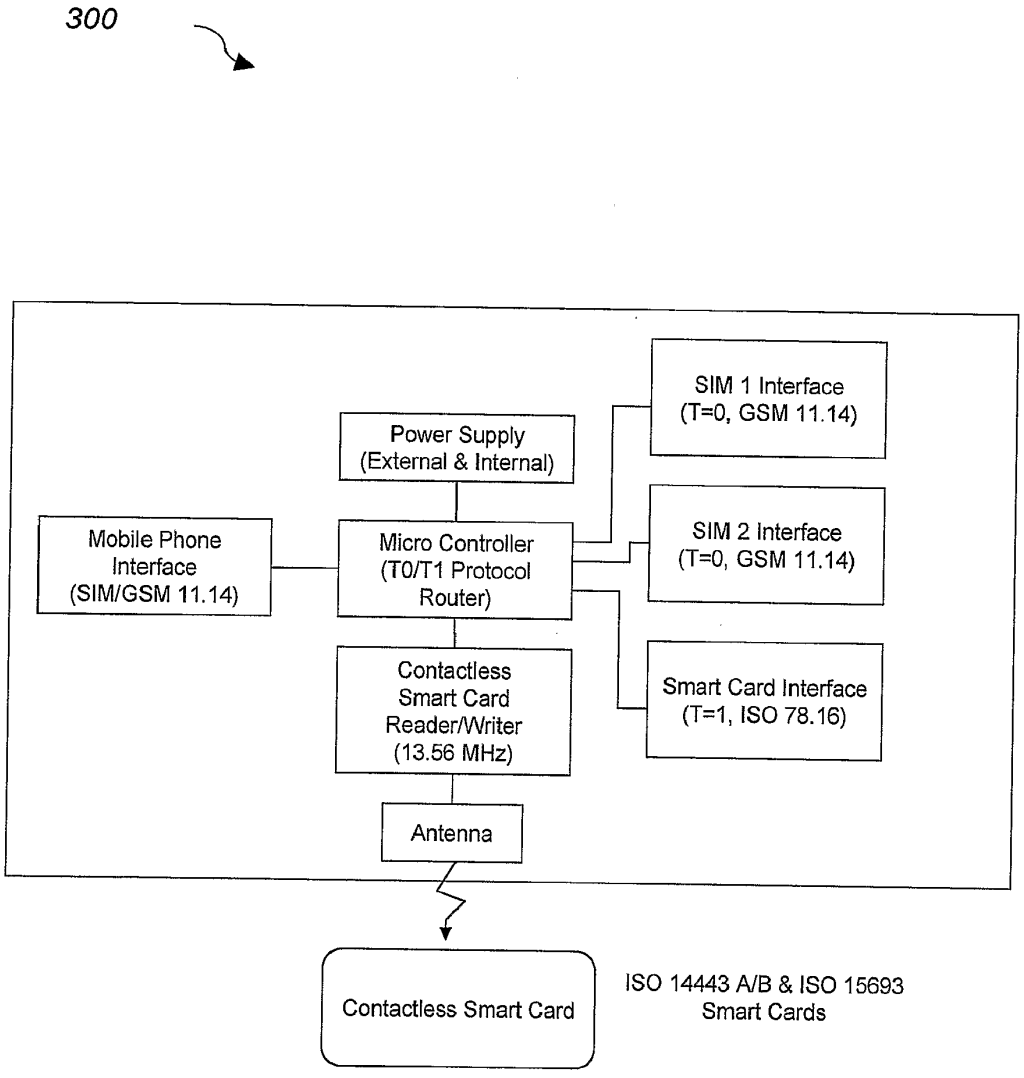

300
SIM 1 Interface
(T=0, GSM 11.14)
Power Supply
(External & Internal)
Mobile Phone
Interface
(SIM/GSM 11.14)
Micro Controller
(T0/T1 Protocol
Router)
SIM 2 Interface
(T=0, GSM 11.14)
Contactless
Smart Card
Reader/Writer
(13.56 MHz)
Smart Card Interface
(T=1, ISO 78.16)
Antenna
Contactless Smart Card
ISO 14443 A/B & ISO 15693
Smart Cards

FIG. 3

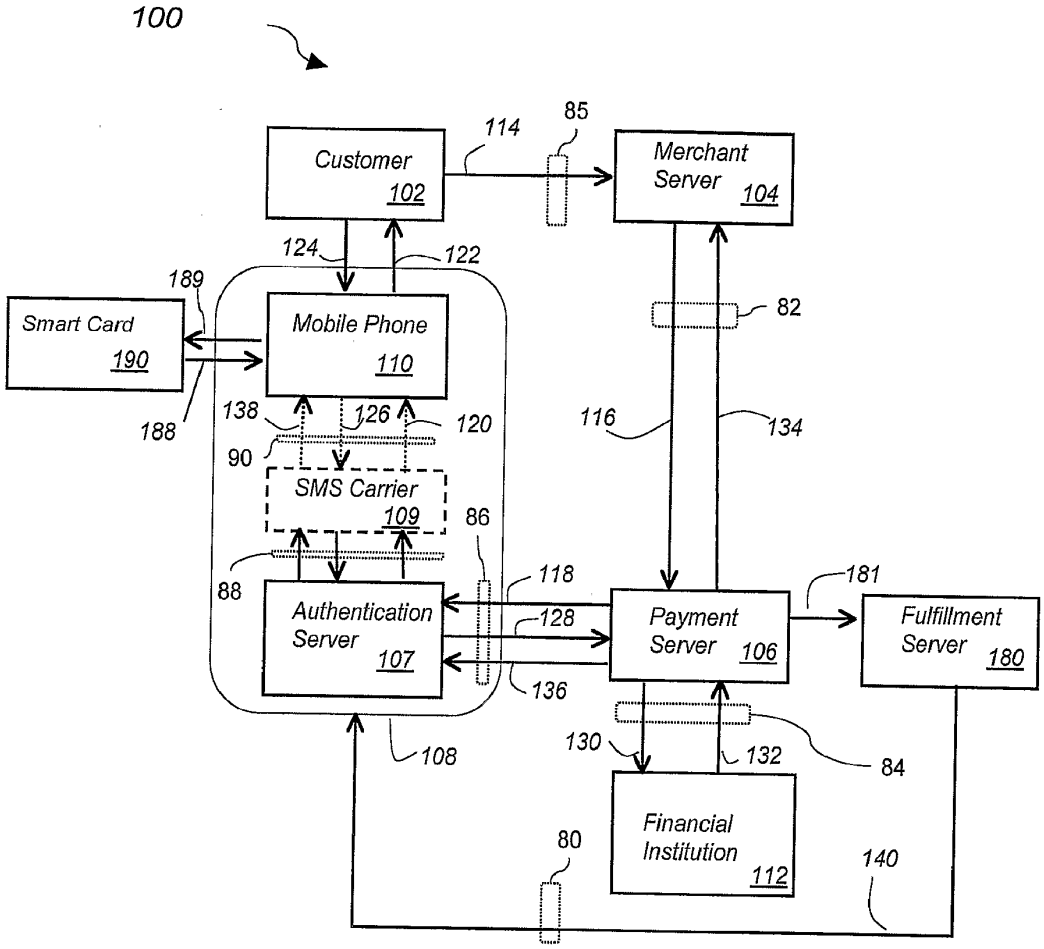

100
Customer 102
Merchant Server 104
Smart Card 190
Mobile Phone 110
SMS Carrier 109
Authentication Server 107
Payment Server 106
Fulfillment Server 180
Financial Institution 112
85
114
124
122
189
82
188
138
126
120
116
134
90
86
88
118
181
128
136
108
130
132
84
80
140

FIG. 4

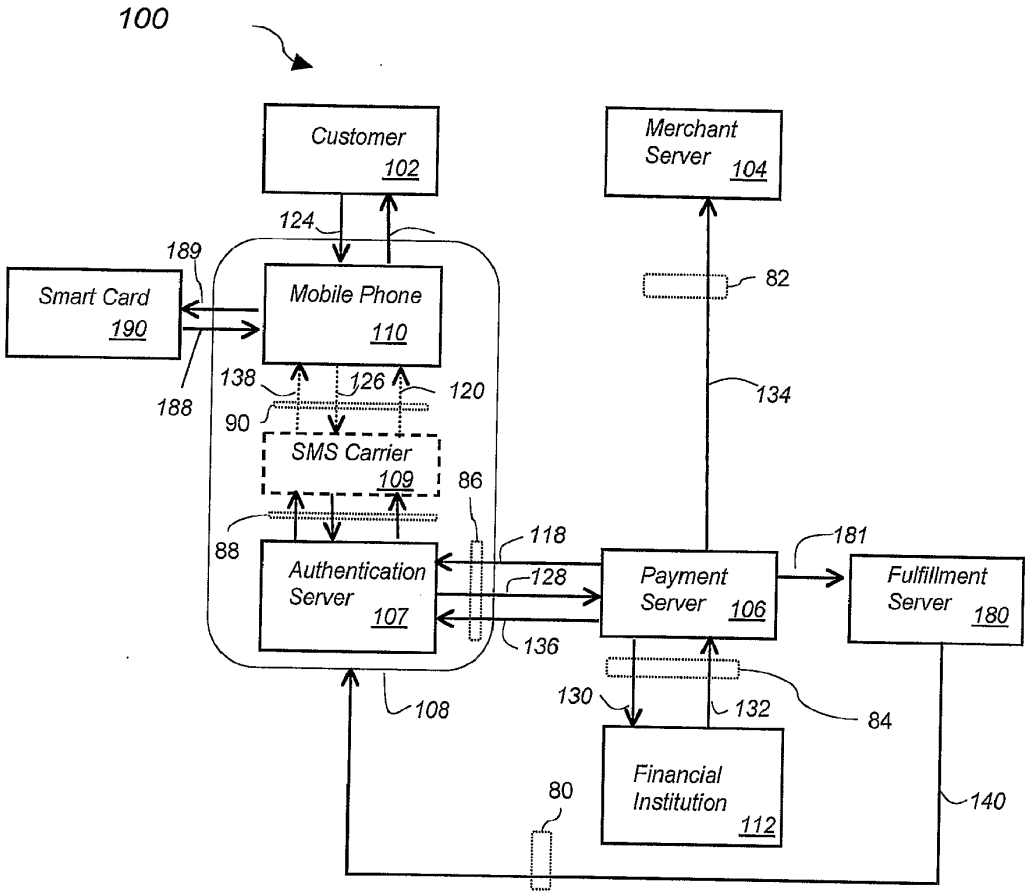

100
Customer 102
Merchant Server 104
124
189
Smart Card 190
Mobile Phone 110
82
138
126
120
188
90
134
SMS Carrier 109
86
88
118
181
Authentication Server 107
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
140

FIG. 4A

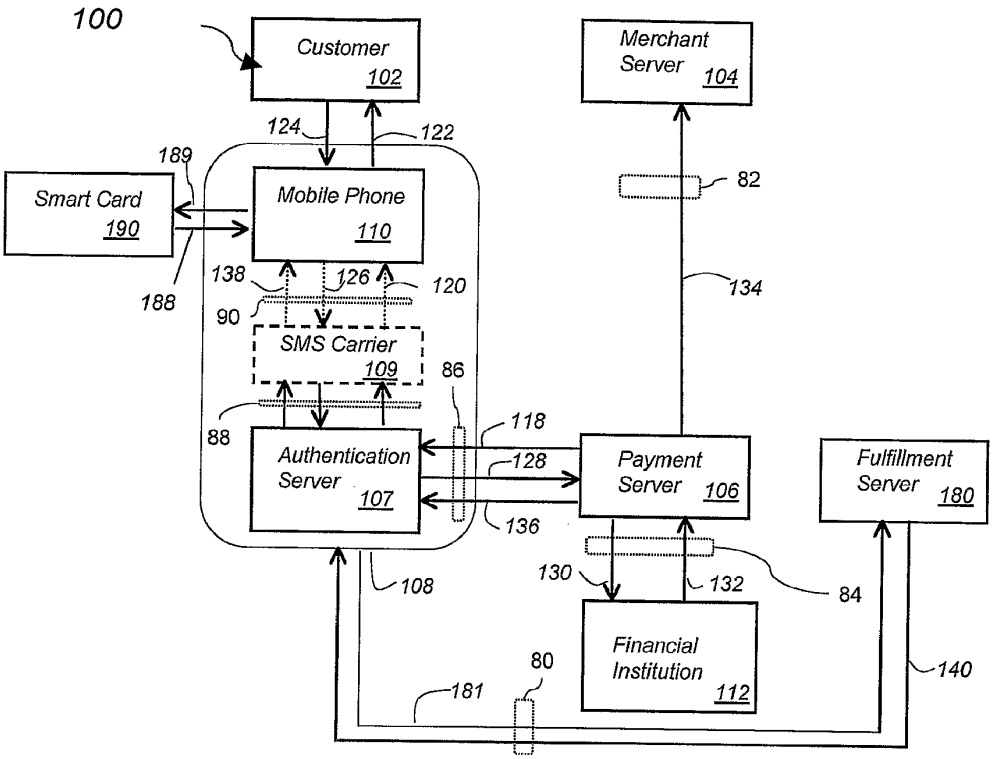

100
Customer 102
Merchant Server 104
124
122
189
Smart Card 190
Mobile Phone 110
82
138
126
120
188
90
SMS Carrier 109
134
86
88
Authentication Server 107
118
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
181
140

FIG. 4B

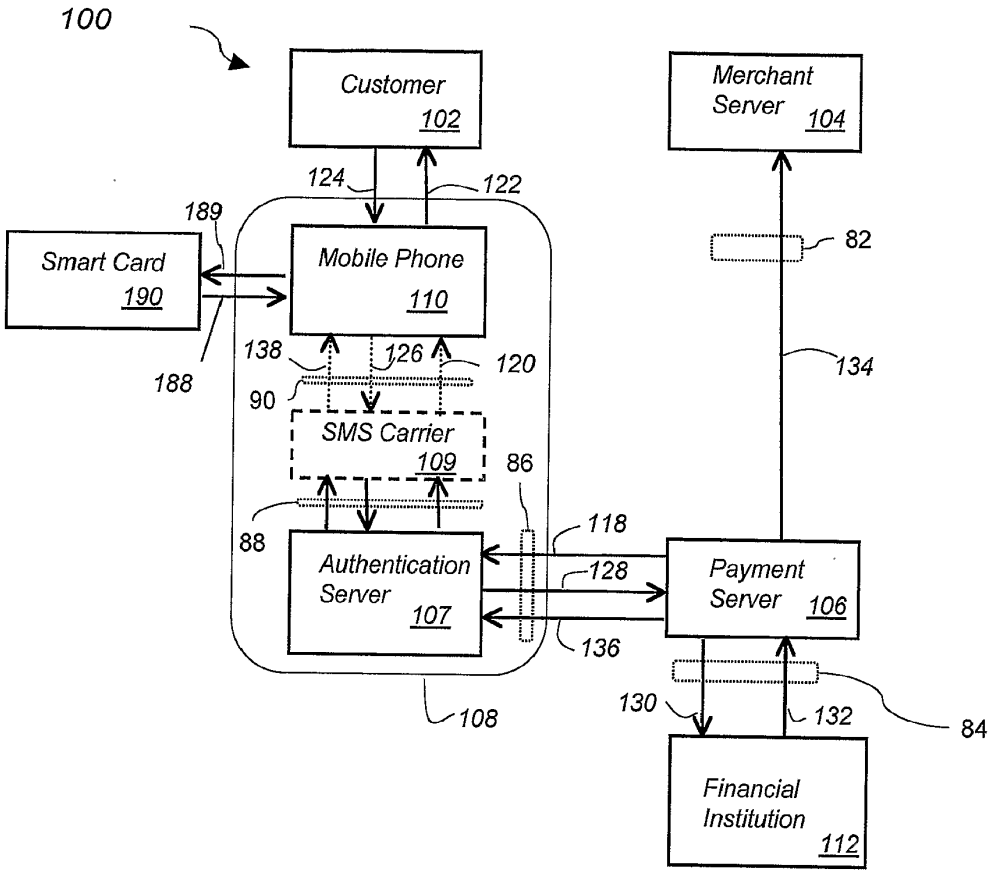

100
Customer
102
Merchant
Server
104
124
122
189
Smart Card
190
Mobile Phone
110
82
138
126
120
188
90
SMS Carrier
109
134
86
88
118
Authentication
Server
107
128
Payment
Server
106
136
130
132
84
108
Financial
Institution
112

FIG. 4C

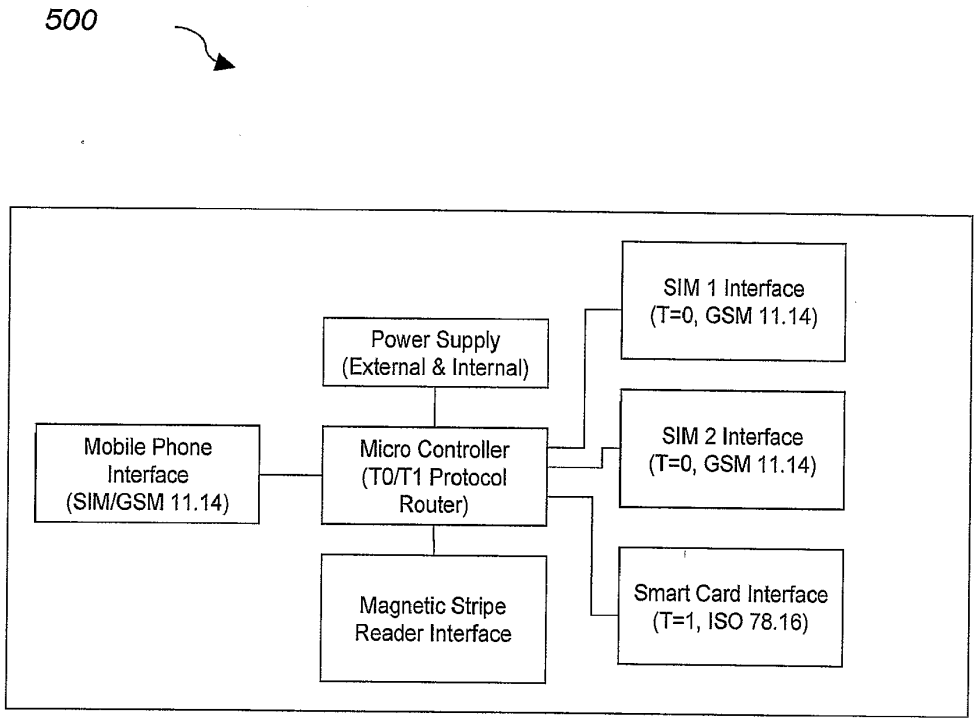

500
SIM 1 Interface
(T=0, GSM 11.14)
Power Supply
(External & Internal)
SIM 2 Interface
(T=0, GSM 11.14)
Mobile Phone
Interface
(SIM/GSM 11.14)
Micro Controller
(T0/T1 Protocol
Router)
Smart Card Interface
(T=1, ISO 78.16)
Magnetic Stripe
Reader Interface

FIG. 5

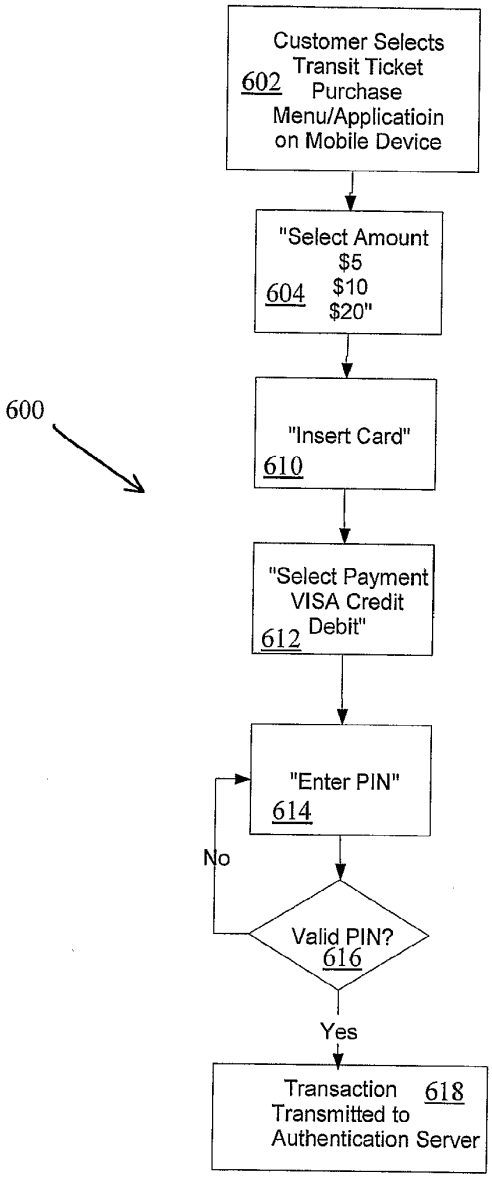
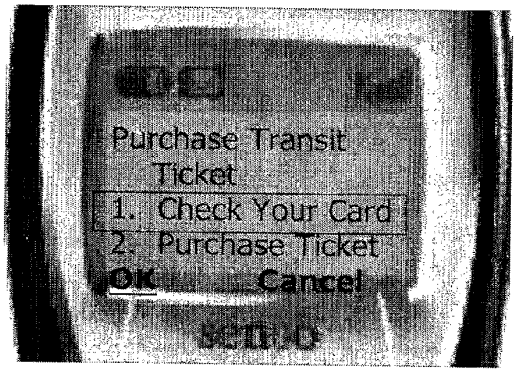
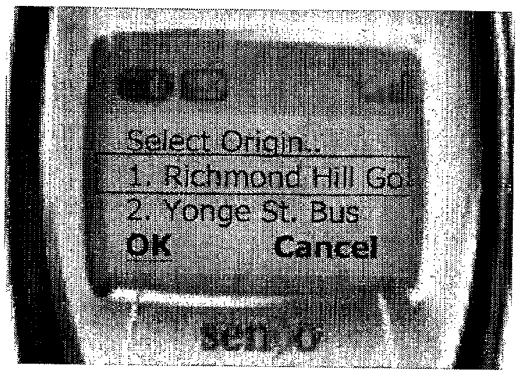

600
Customer Selects Transit Ticket Purchase Menu/Applicatioin on Mobile Device
602
"Select Amount $5 $10 $20"
604
"Insert Card"
610
"Select Payment VISA Credit Debit"
612
"Enter PIN"
614
No
Valid PIN?
616
Yes
Transaction Transmitted to Authentication Server
618

FIG. 6



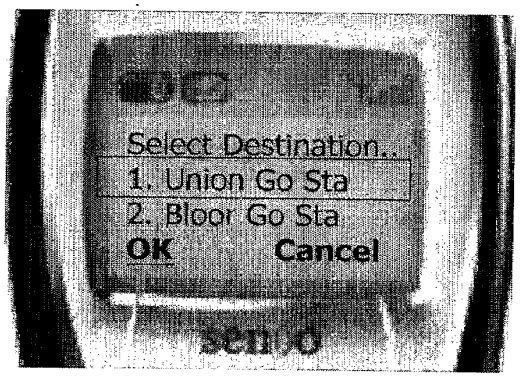
Customer chooses the Purchase Ticket option from the Phone's GO Transit Menu.

FIG. 6A



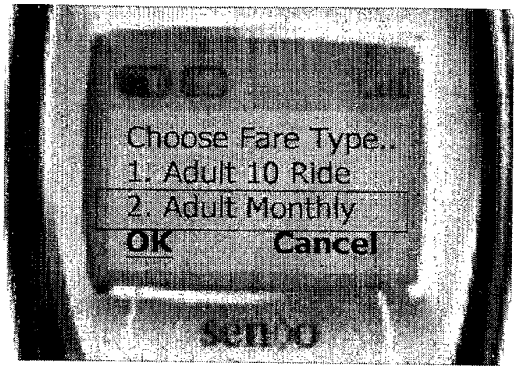
Customer Selects Origin...

FIG. 6B



Customer Selects Destination...

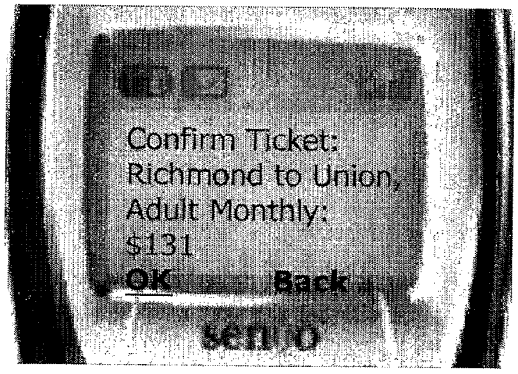
FIG. 6C



607

Customer chooses fare type...

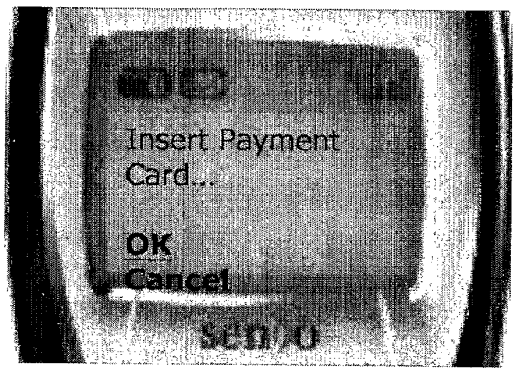
FIG. 6D



608

Fare is calculated and customer confirms ticket purchase

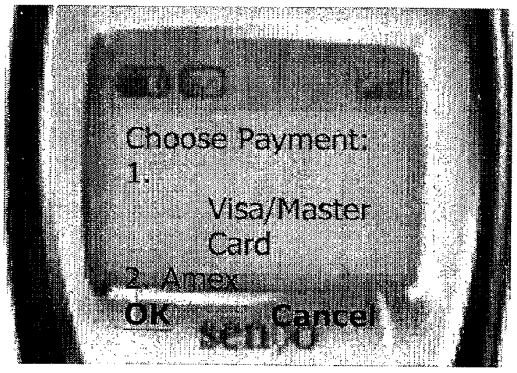
FIG. 6E



610

Customer Initiates Payment and Inserts Payment Card

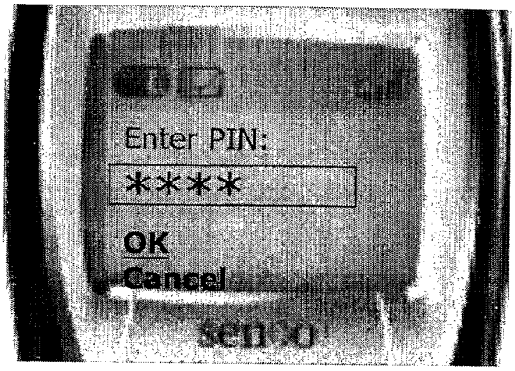
FIG. 6F



612

Customer Selects Payment Instrument on Card

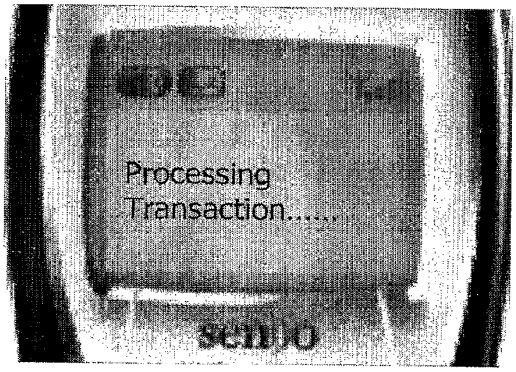
FIG. 6G



614

Customer Authenticates transaction with Personal Identification Number (PIN)

FIG. 6H



618

Transaction Transmitted to Authentication Server and then processed by Merchant, Financial Institution and Fulfillment Server

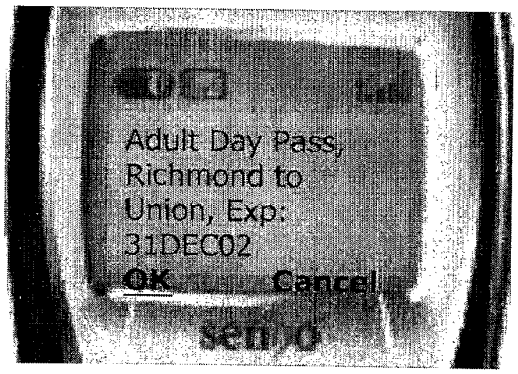
FIG. 6I

Customer presents transit card to the mobile phone

FIG. 6J

Digital Goods are fulfilled to the Transit Card

FIG. 6K



624

Digital Goods fulfillment is completed

FIG. 6L

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/088641 A2

(51) International Patent Classification[7]: G11B

(21) International Application Number:
PCT/US2004/009149

(22) International Filing Date: 25 March 2004 (25.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/457,716	26 March 2003 (26.03.2003)	US
Not furnished	25 March 2004 (25.03.2004)	US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

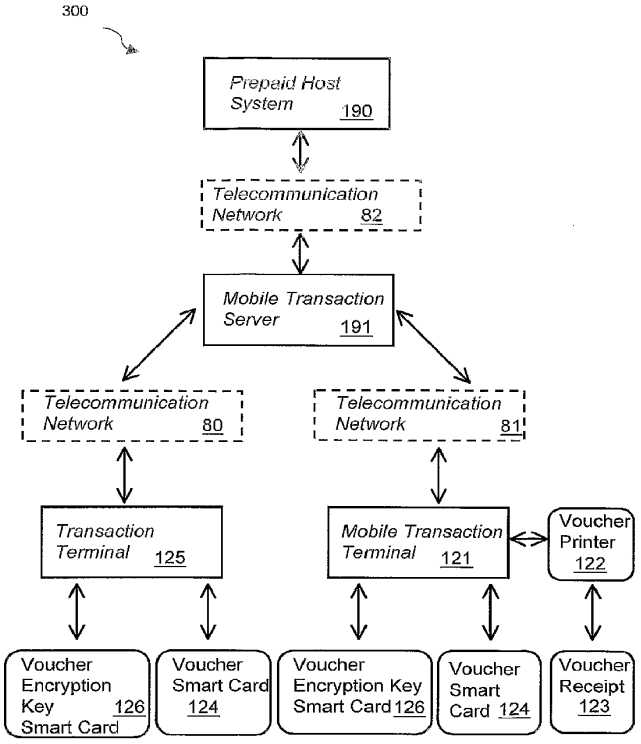
(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **BALSAN, Damien** [US/US]; 78 Melrose Street, Arlington, MA 02474 (US).

(74) Agent: **COLLINS, Aliki, K.. ph. d.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS



(57) Abstract: The present invention describes a system and a method that utilizes transaction terminals (125, 121) equipped with smart card readers to download and store a batch of multiple prepaid electronic vouchers to a smart card (124), retrieve and decrypt individual prepaid vouchers from the smart card and print a voucher receipt with a printer (122) in connection with the transaction terminal. The transaction terminals (125, 121) are in connection with a mobile transaction server (191) that acts as a gateway to a prepaid system (190) and routes transactions between transaction terminals and the prepaid system and between transaction terminals. The present invention also describes a method for storing a voucher encryption key on a second smart card or hardware security module. The voucher encryption key is utilized to decrypt encrypted vouchers on a voucher repository smart card. The present invention also describes a method of transferring encrypted vouchers between voucher smart cards using a single transaction terminal or multiple transaction terminals. The transaction terminals may be mobile devices communicating to the mobile transaction server over wireless networks or computers connected to a wired network.

WO 2004/088641 A2

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/457,716 filed on March 26, 2003 and entitled SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS, which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, and 10/695,585, filed on July 26, 2002, July 23, 2003, and October 28, 2003, and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", and "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for securely storing prepaid top up vouchers on a smart card and utilizing mobile devices to generate the vouchers at the time of purchase.

Background of the Invention

The market for mobile/wireless phone usage has rapidly expanded to reach over 1 billion subscribers throughout the world by the end of 2002. Over 60% of these subscribers prepay for mobile phone usage. The greatest growth of mobile phone subscribers occurs in economically underdeveloped and emerging economies, where it is also common to prepay for many other recurring services, such as utility bills, due to the lack of consumer credit infrastructure.

Referring to FIG. 1 and FIG. 2, a prior art method 100 for prepaying for mobile phone services includes the following steps. First, a customer 110 pays a merchant 120 (111) and receives a scratch card 160 in return (112). Scratch card 160 includes a hidden authorization code 180 covered with a protective coating 170. Customer 110 removes the protective coating 170 using a coin or fingernail to reveal the hidden authorization code 180. Authorization code 180 is also referred to as a "hidden recharge number" (HRN) or a "voucher" or a "voucher number". Next, customer 110 contacts a mobile operator 130 and provides the mobile operator 130 with the authorization code 180 through the mobile operator's call center or an interactive voice response system (113). Mobile operator 130 validates the authorization code 180, "recharges" or "tops up" customer's mobile account with the value associated with the authorization code 180, and notifies customer 110 upon completion of the top up transaction (114). The merchant 120 purchases scratch cards in bulk in multiple denominations for multiple mobile operators 130 from either a scratch card distributor 150 (115) or a wholesaler 140 (118). Typically wholesaler 140 purchases mobile airtime minutes in bulk in advance from several mobile operators 130 (117), manufactures the scratch cards 160 and sells the cards either directly to merchants 120 (118) or through a distributor 150 (116). Typically, merchants 120 are convenience stores, department stores or supermarkets that sell many other types of consumer merchandise. In one example, merchant 120 is a Sam's Club and scratch card 160 is an AT&T phone card. Although this is the most widely used method for topping up mobile phone accounts, the costs associated with scratch card manufacturing, distribution, inventory and potential fraud result in reduced profitability for the mobile operator 130. These costs could represent up to 30% of the face value of the scratch card 160. For example for a typical scratch card 160 with a face value amount of $100, the mobile operator only realizes about $70 in revenue due to the above mentioned costs associated with scratch cards.

Dedicated Point of Sale (POS) terminals and Automated Teller Machines (ATMs) are also used to provide a more cost effective way to top up mobile prepaid accounts by electronically generating and printing the voucher at the time of the purchase. Referring to FIG 3, a prior art method 200 for topping up mobile prepaid accounts includes the following steps. First, customer 110 pays merchant 120 (211). Merchant 120 engages a Point of Sale (POS) Terminal 121 to connect over a telecommunication

network 80 to a remote prepaid system 190 (210, 215). Merchant 120 generates a voucher number (not shown) and prints the voucher number onto a receipt 123 using a printer 122 that is in connection with the POS terminal 121. Next, merchant 120 provides the customer 110 with the voucher receipt 123 that contains the voucher number (not shown) (212). Next, customer 110 provides the mobile operator 130 with the voucher number printed on the voucher receipt 123 (213), the mobile operator 130 validates the voucher number and tops up the customer's mobile account with the value associated with the voucher number (214). Mobile operator 130 also notifies customer 110 upon completion of top up transaction (214). These electronic vouchers are created "online" one at a time by the POS terminal 121 by connecting to prepaid system 190 for each customer 110. Alternatively, the POS terminal 121 connects to the prepaid system 190 less frequently, downloads a batch of multiple vouchers that are securely stored within the memory of the POS terminal 121 and subsequently generates the electronic vouchers "offline" for each customer 110. The problem with this prior art method is the fact that there are not many POS or ATMs readily available to accommodate the number of transactions and users. Accordingly, there is a need for a low cost alternative for a mobile POS or ATM that can securely, store, generate, transfer and print electronic prepaid vouchers.

Summary of the Invention

In general, in one aspect of this invention features a system for generating and storing one or more prepaid electronic vouchers in a voucher smart card. The system includes a voucher host system adapted to generate the prepaid electronic vouchers and a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in the voucher smart card.

Implementations of this aspect of the invention include the following. The system may further include a transaction server adapted to mediate and aggregate transactions and communications between the voucher terminal and the voucher host system over the network connection. The voucher smart card may be a removable smart card such as a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM)

smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card or combinations thereof. The voucher smart card may be a hardware security module (HSM) such as microprocessors or storage accessories. The voucher terminal may be a wireless communication device equipped with a smart card reader/writer module such as a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer or combinations thereof. The smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The voucher terminal may be a wired communication device equipped with a smart card reader/writer module such as a phone, a wired personal digital assistant (PDA), a point of sale (POS) terminal, a television, a personal computer or combinations. The voucher terminal may be a wireless communication device having a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to the SIM card slot and the smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The network may be the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) or a private communication network. The wireless wide area network (WWAN) may be a Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The communications between the voucher host system and the voucher terminal may have a format such as Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats. The system may also include a printer adapted to connect to the voucher terminal for printing hard copies of the prepaid electronic vouchers. The printer may be connected to the voucher terminal via a wired connection such as a serial connection, a parallel connection, a Universal Serial Bus (USB) connection or a mini USB connection. Alternatively, the printer may connect to the voucher terminal via a wireless connection such as infrared, Bluetooth, 801.1x, or other short-range radio frequency connections. The prepaid electronic vouchers may have data such as a mobile operator code, a voucher number, a voucher expiration date, the voucher number in an

encrypted format, a voucher value, a voucher currency code, a voucher product code, a voucher product description, a voucher owner code, or a voucher owner. The prepaid electronic vouchers may have encrypted data and the system may further include a voucher encryption smart card that has a voucher encryption key for decrypting the encrypted data. The voucher encryption key may be a personal identification number (PIN), a private key, a public key, a symmetric key or an asymmetric key. The decrypting may utilize techniques such as symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI). The voucher terminal may further include a first voucher application and the first voucher application may provide for retrieving of the stored electronic prepaid vouchers from the voucher smart card and printing hard copies of the prepaid electronic vouchers. The first application may further provide decrypting encrypted data stored in the electronic prepaid vouchers. The voucher terminal may further include a second voucher application and the second voucher application may provide transferring one or more of the stored prepaid electronic vouchers from the voucher smart card to another voucher smart card.

In general in another aspect the invention features a method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product. The method includes providing a voucher host system adapted to generate the prepaid electronic vouchers and providing a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in a voucher smart card. Next, placing a purchase order and paying for one of the one or more prepaid electronic vouchers from the voucher terminal to the voucher host system over the network connection. Next, downloading the one prepaid electronic voucher from the voucher host system to the voucher terminal over the network connection and storing the one prepaid electronic voucher in the voucher smart card. Next, retrieving the one prepaid electronic voucher from the voucher smart card and presenting the one prepaid electronic voucher to the merchant and receiving the service or product.

Implementations of this aspect of the invention include the following. The method may further include printing a hard copy of the one prepaid electronic voucher before presenting the one prepaid electronic voucher to the merchant. The electronic prepaid voucher may have encrypted data and the method may further include decrypting the encrypted data by inserting an encryption smart card in the voucher terminal, retrieving an encryption key and using it to decrypt the encrypted data. The method may further include transferring the one prepaid voucher from the voucher smart card to a second voucher smart card or to a second voucher terminal.

Among the advantages of this invention may be one or more of the following. When compared to the scratch card method the advantages to storing vouchers on a smart card instead of printing the vouchers onto scratch cards are cost and security. Although the cost of a smart card is significantly higher than a paper or plastic scratch card, the smart card can be used thousands of times to store vouchers whereas the scratch card is used once by the customer and then discarded. Vouchers represent monetary value and therefore security is extremely important. Storing encrypted voucher numbers on a smart card is inherently more secure than scratch cards for several reasons. Scratch cards themselves have no "built in" securities features and rely on a secure manufacturing, distribution and sales environment. In the event of theft of a batch of scratch cards, the person in possession of the scratch cards needs only to remove the protective coating on the card to access the voucher number, a breach in security can occur at the merchant location or at any point in the scratch card manufacturing and distribution process. Smart Cards, however, have many "built in" security features that establish a tamper resistant environment for securely storing data from logical and physical attacks which is the primary reason that the financial industry is moving away from magnetic stripe cards to smart cards for debit, credit and electronic cash applications and the primary reason that mobile network operators utilize Subscriber Identity Module (SIM) smart cards. In the event of theft of a smart card with vouchers, the person in possession of the smart card would first have to compromise the security of the smart card to access the encrypted vouchers, then compromise the voucher encryption key that may be stored on the same card or on a different card. The expense and time required to successfully carry out such an attack is significantly more costly than the value of the vouchers on the smart card.

When compared to other Point of Sale (POS) voucher methods, the present invention has the advantage of mobility. The existing prior art POS voucher methods store the vouchers within the device but do not separate storage from fulfillment, i.e., one device is used for both purposes. In the present invention, vouchers are stored on a removable smart card that can be used by one device for voucher storage transactions and then removed and inserted into another device for voucher generation and printing. The present invention provides secure mobility for voucher generation and printing enabling one transaction device to store transactions on a smart card and multiple devices can be deployed to service customer needs remotely.

Brief Description of the Drawings

FIG. 1 is a block diagram of a prior art system for prepaying for mobile phone services;

FIG. 2 is a schematic diagram of a prior art prepaid phone scratch card;

FIG. 3 is schematic diagram of a prior art electronic prepaid voucher system;

FIG. 4 is schematic diagram of an electronic prepaid voucher system that utilizes smart cards according to this invention;

FIG. 5 is a flow diagram of a voucher download transaction to a smart card according to this invention;

FIG. 6 is a flow diagram of a voucher generation transaction from a smart card and print transaction according to this invention;

FIG. 7 is a diagram representing the screen flow and application logic of a mobile transaction terminal application according to this invention;

FIG. 8 is a flow diagram of a voucher transfer transaction according to this invention; and

FIG. 9 is a diagram representing the screen flow and application logic of a voucher transfer transaction according to this invention.

Detailed Description of the Invention

The present invention describes a system and a method for using a transaction terminal for downloading and storing prepaid electronic vouchers on a first smart card, retrieving and decrypting prepaid vouchers from the first smart card and printing a voucher receipt in a printer that is connected with the transaction terminal. The present invention also describes a system and a method for storing a voucher encryption key on a second smart card and then using the second card to decrypt encrypted vouchers on the first smart card. The present invention also describes a system and a method of transferring prepaid vouchers between voucher smart cards.

Referring to FIG. 4, a system 300 for downloading and storing prepaid electronic vouchers on a smart card includes a Prepaid Host System 190, a Mobile Transaction Server 191, a Transaction Terminal 125, a Mobile Transaction Terminal 121, a Printer 122, a Voucher Smart Card 124, a Voucher Encryption Key Smart Card 126, and a Voucher Receipt 123. The Prepaid Host System 190 is the primary source for generating voucher information. The Mobile Transaction Server 191 connects to the Prepaid Host System 190 over telecommunication network 82 and to the transaction terminal 125 and the mobile transaction terminal 121 over telecommunication networks 80, and 81 respectively. Mobile Transaction Server 191 functions as a gateway that mediates and aggregates the transactions between the Prepaid Host System 190 and the transaction terminal 125 and the mobile transaction terminal 121. In one example, Voucher Smart Card 124 and Voucher Encryption Key Smart Card 126 are removable smart cards including "full-size" smart cards, such as credit cards, debit cards, contactless smart cards, stored-value cards, coupon cards, reward cards, electronic cash cards, loyalty cards, identification cards and secure access application or "plug in" format smart cards like those used for Subscriber Identity Modules (SIM's) smart cards utilized by mobile telephones or Secure Access Modules (SAM's) smart cards utilized by Point of Sale (POS) devices. In another example Voucher Smart card 124 and Voucher Encryption Card are hardware security modules (HSM) including accessories that are added to computers, servers and Personal Digital Assistants (PDA's) for banking and secure access applications and secure

microprocessors that are utilized by Point of Sale (POS) devices. Voucher Encryption Key smart cards have the ability to securely store data and resist tampering and can generate cryptographic keys and encrypt/decrypt data utilizing a cryptographic co-processor. Telecommunications networks 80, 81 and 82 can be the Internet, a public telecommunication network, a private telecommunication network, a local area network (LAN) wireless wide area network (WWAN), a wireless local area network (WLAN) or a personal area network (PAN). The data exchanged using telecommunications networks 80, 81 and 82 have a format such as Short Message Service (SMS), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), or Simple Network Management Protocol (SNMP) over Transmission Control Protocol/Internet Protocol (TCP/IP). Transaction Terminal 125 and Mobile Transaction Terminal 121 are capable of receiving a voucher smart card and printing a voucher receipt 123 via a printer 122 (not shown for Terminal Transaction 125).

Referring to FIG. 10, in one example, the transaction terminal 125 is a mobile phone that is capable of receiving smart cards 902, 903, 904 as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", the entire content of which is incorporated herein by reference. In other examples, the transaction terminal 125 is a Point of Sale terminal equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. Similarly, the mobile transaction terminal 121 is a mobile phone as shown in FIG. 10 equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. In another example, the mobile transaction terminal 121 is a smart card reader equipped with a keypad and a display.

A merchant utilizes the present invention to sell prepaid vouchers to consumers, and the consumers use this invention to recharge their prepaid account. For example, at the beginning of each day, the merchant uses the transaction terminal device described in this invention to connect to a prepaid host system and download a batch of prepaid vouchers in various denominations to a smart card. The merchant may be a small convenient storeowner, a large supermarket sales clerk, an independent sales representative or a sales representative working for a telecommunication company.

Throughout the day the merchant sells the prepaid vouchers to customers who are interested in purchasing a voucher. The customers pay the merchant with cash, credit or debit card. Alternatively, a customer approaches the merchant for purchasing a voucher. The merchant uses the transaction terminal device of this invention to retrieve a voucher from the smart card and prints a receipt for the customer with the voucher number on it. The customer then contacts his service provider and gives the voucher number to the service provider at which point the service provider validates the voucher number and "tops up' or "recharges" the customer's account. The voucher numbers are encrypted on the smart card. The encryption key required to decipher the encrypted information is stored on another smart card. Both cards, i.e., the smart card with the encrypted voucher number and the smart card with the encryption key, need to be present in the transaction terminal device of this invention in order to decrypt, retrieve and present a voucher number for the customer. This process of batch downloading and individual retrieving of vouchers may be distributed among several individuals. For example, a sales manager may download batches of vouchers to multiple smart cards and give each smart card to individual sales representatives. The sales manager may utilize separate smart cards for individual prepaid products, i.e. one card for a mobile operator and another smart card for a long distance telecommunication provider. The sales manager may require the individual sales representatives to pay a deposit or the full amount of value of the vouchers stored on the smart card in advance. Throughout the day, as the sales representatives deplete their inventory the sales manager may also transfer additional vouchers to sales representatives remotely using the transaction terminal device and system described in the present invention. At the end of the day, the sales representatives return their smart cards to the sales manager at which point the sales representatives and the merchant reconcile the financial transactions. Alternatively, the financial settlement may occur remotely and electronically.

Referring to FIG. 5, the process of downloading a voucher includes the following steps. First, the transaction terminal 125 establishes a connection with the mobile transaction server 190 over network 80 (410). Next, mobile transaction server 191 routes the transaction request to the prepaid host system 190 through network 82 (411). The prepaid host system 190 validates the connection and transmits a specified

quantity and types of vouchers to the mobile transaction server 191 over network 82 (412). The mobile transaction server 191 routes the downloaded vouchers to the transaction terminal 125 through network connection 80 (413). In one example, the data in the voucher download transaction for a single voucher include, a code representing the mobile operator that the voucher is associate with, a voucher serial number, a voucher expatriation date, the voucher number in its encrypted format, the voucher value and a code representing the currency of the voucher value. Upon completion of the voucher download transaction, the transaction terminal 125 transmits a transaction complete acknowledgement to the mobile transaction server 191 through network connection 80 (416) and the mobile transaction server 191 transmits this acknowledgement to the prepaid host system 190 over network 82 (417). The transaction terminal 125 is in connection with a voucher smart card 124 and sends the voucher data to the voucher smart card 124 (414). Upon completion of the transaction the transaction terminal 125 receives an acknowledgement from the voucher smart card 124 (415). In one embodiment, the Prepaid Host System 190 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125. In this embodiment the connection is initiated by the prepaid host system 190 (408, 409). In another embodiment, the Transaction Terminal 125 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125.

Referring to FIG. 6 and FIG. 7, a method 500 for retrieving a voucher from a smart card 124 and printing a voucher receipt 124 includes the following steps. First, a user utilizes a mobile transaction application 600 stored on the mobile transaction terminal 121 to start a new transaction (610). The user is then prompted to insert the voucher smart card 124 into the mobile transaction terminal 121 (612). The mobile transaction application 600 on the mobile transaction terminal 121 accesses the voucher smart card 124 (517) and retrieves the inventory of available vouchers (518). The inventory of available mobile operators is displayed on the mobile transaction terminal application and the user is prompted to make a selection (614). Following the selection of a specific mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (616). Following the selection of a specific voucher, the user is prompted to confirm the selection (618). Upon confirmation, the mobile transaction application

600 accesses voucher smart card 124 (519), retrieves the voucher data associated with the confirmed selection (520), updates the inventory on the voucher smart card 124 (521) and stores the voucher data within the memory (not shown) of the mobile transaction terminal 121. Next, the mobile transaction application 600 accesses the voucher encryption key smart card 126 (510), and if the mobile transaction terminal 121 is not in connection with the voucher encryption key smart card 126, the user is prompted to insert the voucher encryption key smart card 126 (620). The mobile transaction application 600 accesses the voucher encryption key smart card 126 to retrieve smart card profile information (511). If the mobile transaction terminal 121 is configured to receive only one smart card, the user is asked to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (622). The users types the PIN and the mobile transaction application 600 presents the PIN to the voucher encryption key smart card 126 (512) for authorization. The authorization result is returned to the mobile transaction application 600 (513) and upon successful authorization, the mobile transaction application 600 retrieves the voucher encryption key (not shown) (514). The voucher encryption key is utilized by the mobile transaction application 600 to decrypt the encrypted voucher information that was previously retrieved by the mobile transaction application 600 from the voucher smart card 124. The decryption process (not shown) utilizes symmetric keys or asymmetric keys and cryptographic techniques such as Data Encryption Standard (DES, 3DES), RSA, Elliptical Curve Cryptography (ECC), Message Authentication Codes (MAC, HMAC), SHA-1, AES and Public Key Infrastructure (PKI). When the voucher decryption is completed, the user is prompted to either print or view the decrypted voucher information on the screen (626). The mobile transaction terminal 121 is in connection with a printer 122. Communication 70 with the printer 122 is either wired (i.e. serial, parallel, USB) or wireless (i.e. infrared, Bluetooth, 802.1x). If the user selects the print option, the mobile transaction terminal 121 establishes connection 70 with the printer 122 and sends the voucher data to the printer (522). The printer 122 formats the voucher data accordingly, generates voucher receipt 123 (524) and acknowledges results of print process to the mobile transaction terminal 121 (523). Alternatively, the user selects to present the voucher data on the display (not shown) of the mobile transaction terminal

121. The mobile transaction application 600 reestablishes connection with the voucher smart card 124 to update the voucher inventory with the completed transaction details (525). Once a voucher is retrieved, the voucher is either deleted from the inventory or its status is changed such that it can no longer be retrieved.

The present invention also defines a process for transferring vouchers between voucher smart cards. In one case, the voucher transfer process is local and it uses the same transaction terminal (mobile or otherwise) to transfer vouchers from one voucher smart card to another voucher smart card. In another case the voucher transfer process is remote and it uses one transaction terminal (mobile or otherwise) to transmit voucher data to another transaction terminal (mobile or otherwise). Referring to FIG. 8 and FIG. 9, using voucher transfer application 800, a user initiates a voucher transfer transaction 700. The user is prompted to insert the origin voucher smart card 124 that stores the vouchers into the transaction terminal 125. The voucher transfer application 800 accesses voucher smart card 124 (717) and retrieves the inventory of available vouchers (718). The inventory of available mobile operators is displayed on the transaction terminal application and the user is prompted to make a selection (814). Following the selection of a mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (816). Following the selection of a voucher value, the inventory of available vouchers for the selected operator and value denominations are displayed and the user is prompted to select a quantity of vouchers that is less than or equal to the total quantity of vouchers available (818). Following the selection of one or more vouchers, the use is prompted to confirm the selection (819). Upon confirmation, the voucher transfer application 800 accesses voucher smart card 124 (719), retrieves the voucher data associated with the confirmed selection (720), updates the inventory on the voucher smart card 124 and stores the voucher data within the memory (not shown) of the transaction terminal 125 (721). In one example, the transfer of vouchers requires authorization. If the transaction terminal 125 is configured to receive only one smart card, the user is required to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (822). The users types the PIN, the voucher transfer

application 800 presents the PIN to the voucher encryption key smart card 126 for authorization (712) and the authorization result is returned to the voucher transfer application 800 (713). Upon successful authorization, the voucher data are transferred from the memory (not shown) of the transaction terminal 125 to a temporary storage repository on the voucher encryption key smart card 126 (714) and then the user is prompted to choose the transfer method (824). The transfer method is either a local "card to card" transfer or a remote transfer. If the user selects the local "card to card" transfer option, the user is prompted to insert the destination voucher smart card 124a (828). The voucher transfer application 800 retrieves the voucher data from the temporary storage repository on the voucher encryption key smart card 126 (715) and appends the voucher data to the destination voucher smart card 124a (722). After receiving the voucher data, the destination voucher smart card 124a provides an acknowledgement response to the transaction terminal application (723) that is further routed to the voucher encryption key smart card 126 to complete the card transfer transaction (716). If the transaction terminal is configured to receive only one smart card, the user is prompted to remove and insert the origin voucher smart card 124, the voucher encryption key smart card 126 and the destination voucher smart card 124a in the appropriate sequence to complete the transaction (830). If the user selects the remote transfer option, the user is prompted to enter the Identification Number of the destination transaction terminal (826). The voucher transfer application 800 transmits the voucher data to the mobile transaction server 191 over network 80 (724). Mobile transaction server 191 transmits an acknowledgment of the receipt of the voucher data over network 80 to transaction terminal 125 which is then routed to the voucher encryption key smart card 126 to complete the transaction from the origin of the transfer (716). The mobile transaction server 191 transmits a notification to the mobile transaction terminal 121 designated by the origin 826 over network 81 (726). The mobile transaction terminal 121 receives the notification (726) and transmits an acknowledgement and a download request from the mobile transaction server 191 over network 81 (727). The mobile transaction server 191 transmits the voucher download to mobile transaction terminal 121 over network 81 (728). The user is prompted to insert the voucher smart card 124b and a voucher transaction application 800a on the mobile transaction terminal 121 appends the voucher data to the destination voucher smart card 124b (729). A voucher data transfer acknowledgement is transmitted to the mobile transaction

terminal 121(730) and routed to the mobile transaction server 191 over network 81 to complete the remote transfer transaction (731).

In another embodiment, the transaction terminal (mobile or otherwise) is also a payment terminal that enables the user to accept and process electronic payments as described in a co-pending patent application entitled "System and method for payment transaction authentication", the entire content of which is incorporated herein by reference. In another embodiment, the transaction terminal (mobile or otherwise) is also configured to receive magnetic stripe payment cards as described in a co-pending patent application entitled "Mobile Communication Device Equipped with a Magnetic stripe Reader". In another embodiment, the mobile transaction terminal 121 has no connection to the mobile transaction server. The voucher encryption key smart card 126 and the voucher smart card 124 l store all transaction information that is transferred to another transaction terminal utilizing the "card to card" transfer method described in FIG. 8 and FIG. 9. In another embodiment, the Prepaid Host System 190 is any type of service that utilizes vouchers such as utilities, local phone service, long distance phone service, pay-per-view entertainment, electronic ticketing. In another embodiment, the encrypted vouchers are stored in the memory of the mobile transaction terminal 121 or transaction terminal 125. The memory is either internal to the mobile device or external and in connection with the mobile device (i.e. Compact Flash, Secure Digital, USB Flash memory, external hard drive). In yet another embodiment, the encrypted vouchers are stored in the memory 901 of the mobile phone attachment as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", shown in FIG. 10. Referring to FIG. 4, in another embodiment the mobile transaction terminal 121 has no network connection 81 with the mobile transaction server 191 and is a non-network connected device with the ability to interact with voucher encryption key smart card 126, voucher smart card 124 and optionally voucher printer 122.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

1. A system for generating and storing one or more prepaid electronic vouchers comprising:

a voucher host system adapted to generate said prepaid electronic vouchers;

a voucher smart card; and

a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in said voucher smart card.

2. The system of claim 1 further comprising a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

3. The system of claim 1 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

4. The system of claim 1 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

5. The system of claim 1 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

6. The system of claim 1 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

7. The system of claim 1 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

8. The system of claim 1 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

9. The system of claim 8 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

10. The system of claim 2 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

11. The system of claim 1 further comprising a printer adapted to connect to said voucher terminal for printing hard copies of said prepaid electronic vouchers.

12. The system of claim 11 wherein said printer is connected to said voucher terminal via a wired connection selected from a group consisting of a serial connection, a parallel connection, a USB connection and a mini USB connection.

13. The system of claim 11 wherein said printer is connected to said voucher terminal via a wireless connection selected from a group consisting of infrared, Bluetooth, 801.1x, and short-range radio frequency (RF) connections.

14. The system of claim 1 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

15. The system of claim 1 wherein said prepaid electronic vouchers comprise encrypted data.

16. The system of claim 15 further comprising a voucher encryption smart card wherein said voucher encryption smart card comprises a voucher encryption key for decrypting said encrypted data.

17. The system of claim 16 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key and an asymmetric key.

18. The system of claim 16 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

19. The system of claim 1 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides retrieving of said

stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

20. The system of claim 19 wherein said first application further provides decrypting encrypted data stored in said electronic prepaid vouchers.

21. The system of claim 1 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

22. A method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product, said method comprising:

providing a voucher host system adapted to generate said prepaid electronic vouchers;

providing a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in a voucher smart card;

placing a purchase order and paying for one of said one or more prepaid electronic vouchers from said voucher terminal to said voucher host system over said network connection;

downloading said one prepaid electronic voucher from said voucher host system to said voucher terminal over said network connection and storing said one prepaid electronic voucher in said voucher smart card;

retrieving said one prepaid electronic voucher from said voucher smart card; and

presenting said one prepaid electronic voucher to said merchant and receiving said service or product.

23. The method of claim 22 further comprising providing a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

24. The method of claim 22 further comprising printing a hard copy of said one prepaid electronic voucher before presenting said one prepaid electronic voucher to said merchant.

25. The method of claim 22 wherein said one electronic prepaid voucher comprises data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

26. The method of claim 22 wherein said one prepaid electronic voucher comprises encrypted data.

27. The method of claim 26 wherein an encryption key for said encrypted data is stored in an encryption smart card.

28. The method of claim 27 further comprising decrypting said encrypted data by inserting said encryption smart card in said voucher terminal, retrieving said encryption key and using it to decrypt said encrypted data.

29. The method of claim 22 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

30. The method of claim 22 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

31. The method of claim 22 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a

pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

32. The method of claim 22 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

33. The method of claim 22 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

34. The method of claim 22 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

35. The method of claim 34 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

36. The method of claim 23 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

37. The method of claim 22 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

38. The method of claim 27 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key, and an asymmetric key.

39. The method of claim 28 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

40. The method of claim 22 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides said retrieving of said stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

41. The method of claim 40 wherein said first application further provides decrypting of encrypted data stored in said electronic prepaid vouchers.

42. The method of claim 40 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

43. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher smart card.

44. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher terminal.

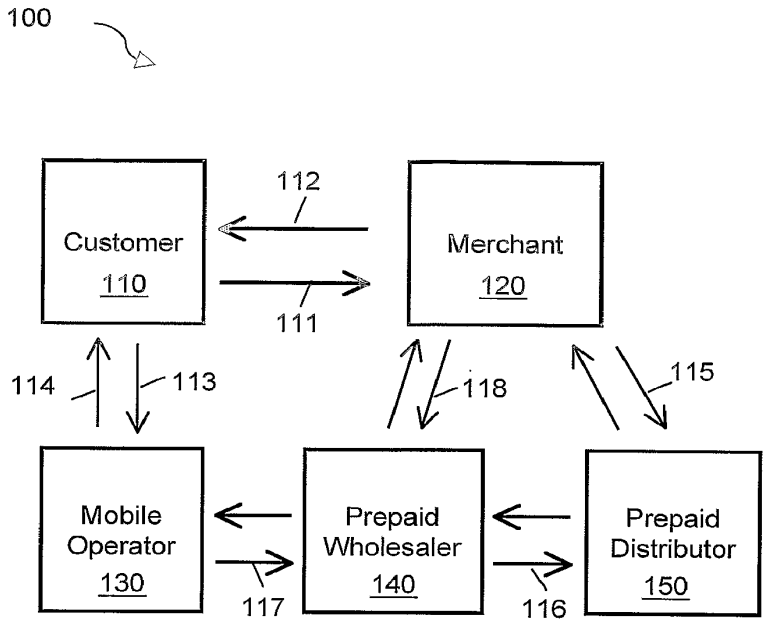


FIG. 1
(Prior Art)

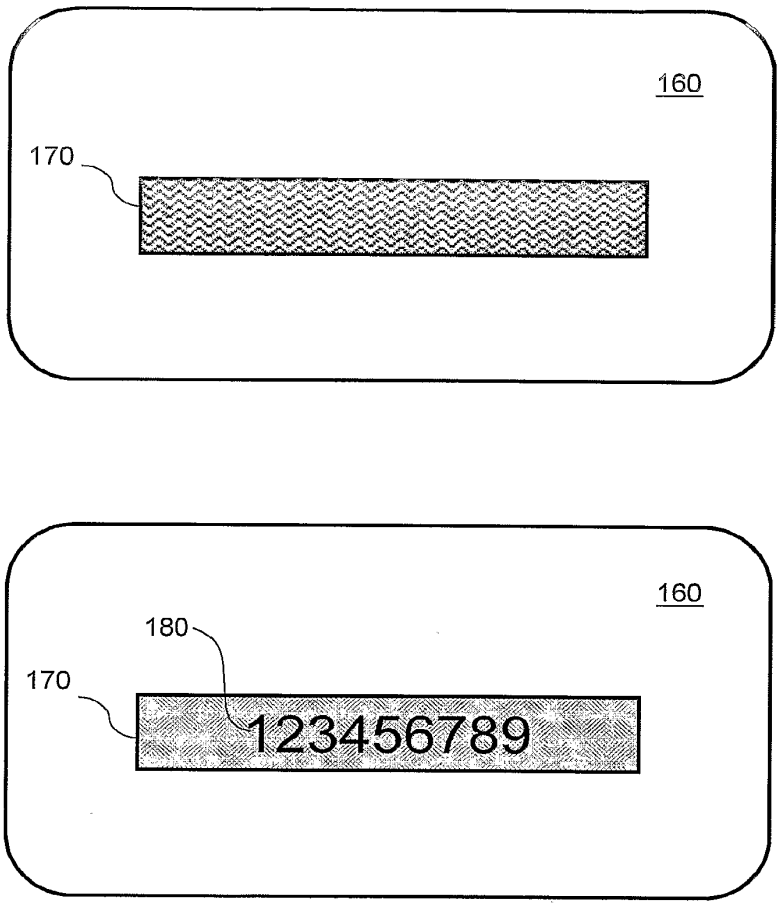


FIG. 2
(Prior Art)

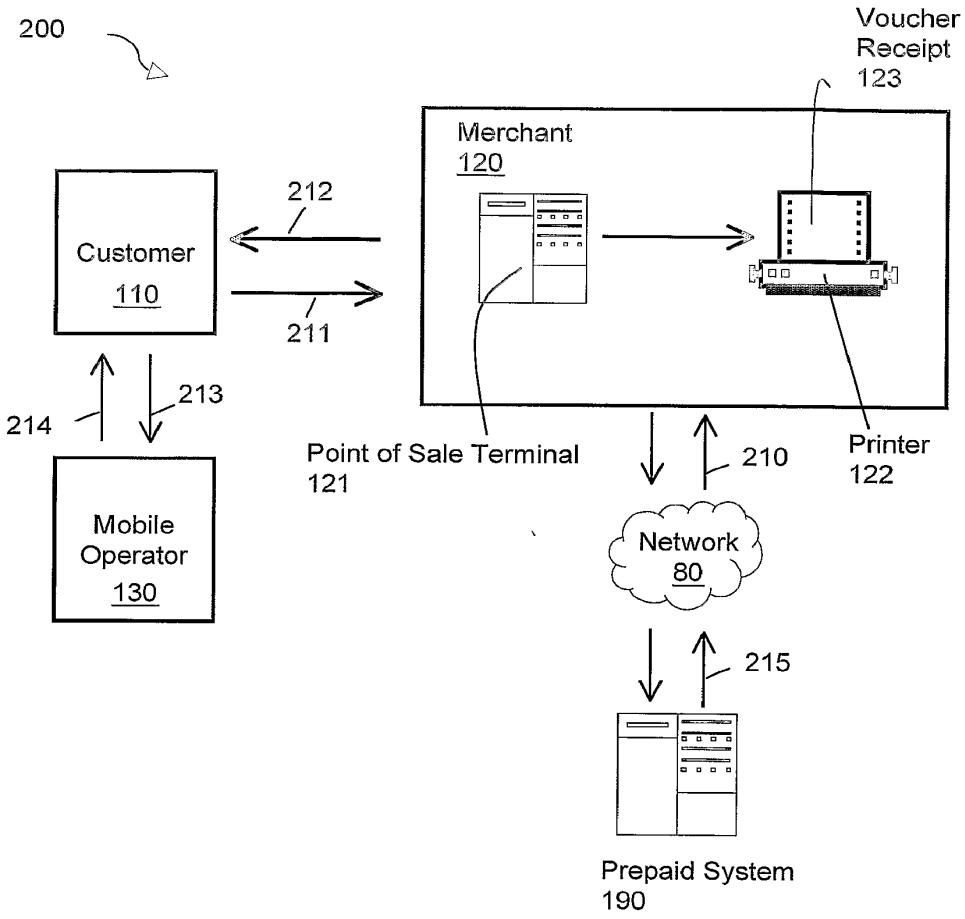


FIG. 3
(Prior Art)

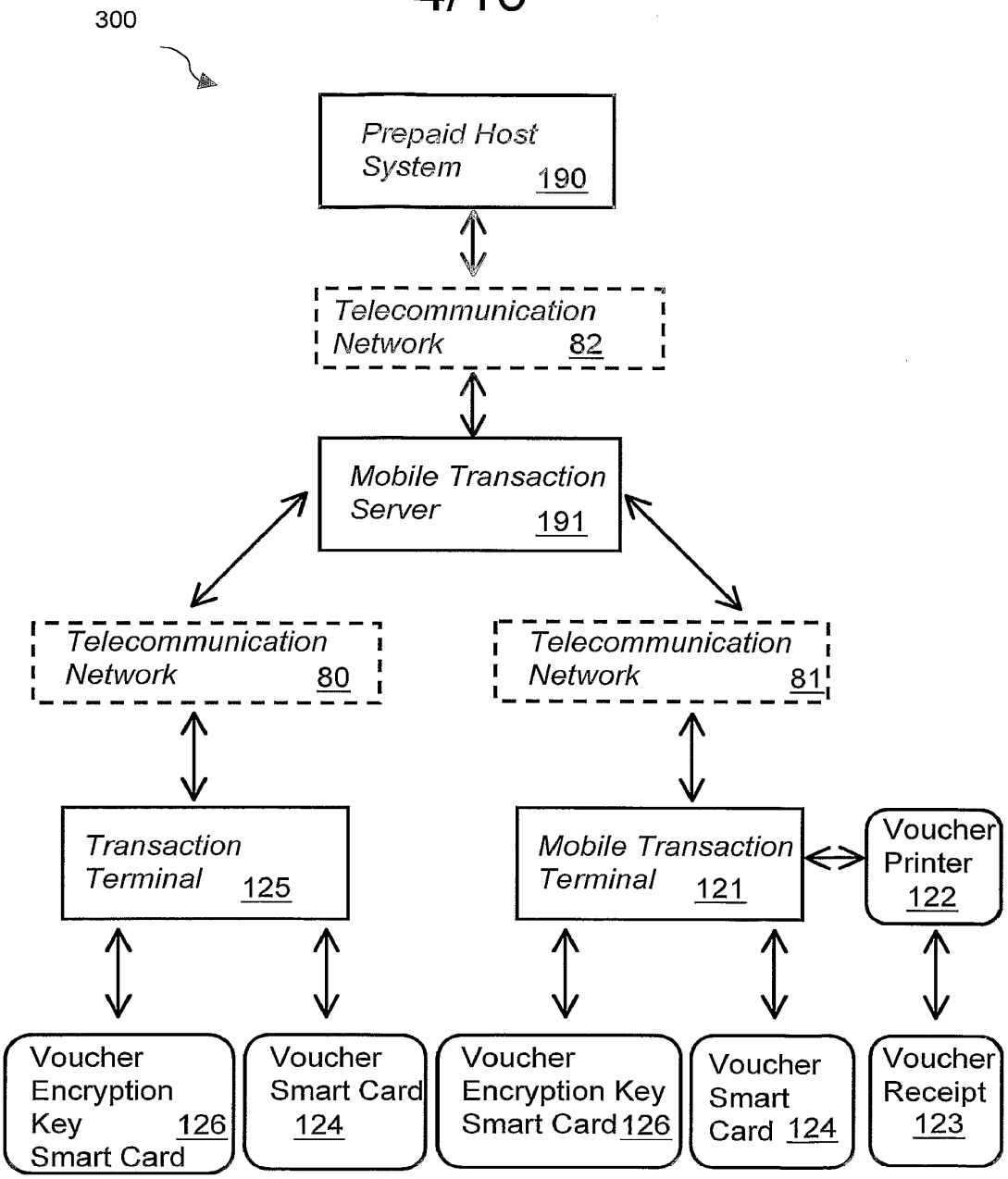

300
Prepaid Host System 190
Telecommunication Network 82
Mobile Transaction Server 191
Telecommunication Network 80
Telecommunication Network 81
Transaction Terminal 125
Mobile Transaction Terminal 121
Voucher Printer 122
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Receipt 123

FIG. 4

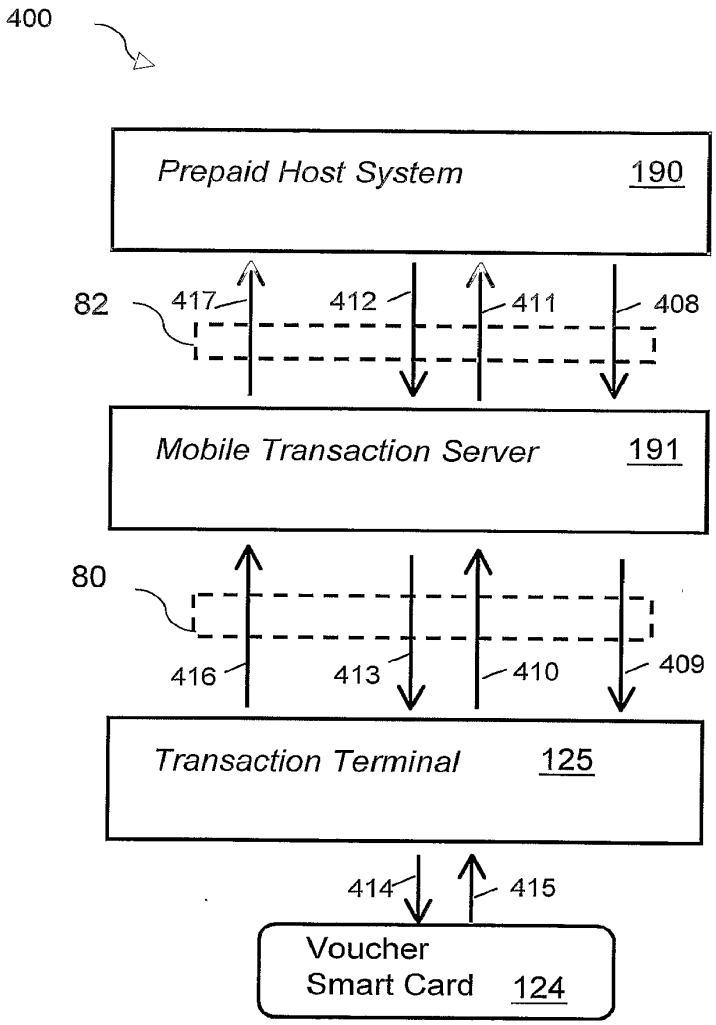

400
Prepaid Host System 190
82
417
412
411
408
Mobile Transaction Server 191
80
416
413
410
409
Transaction Terminal 125
414
415
Voucher
Smart Card 124

FIG. 5

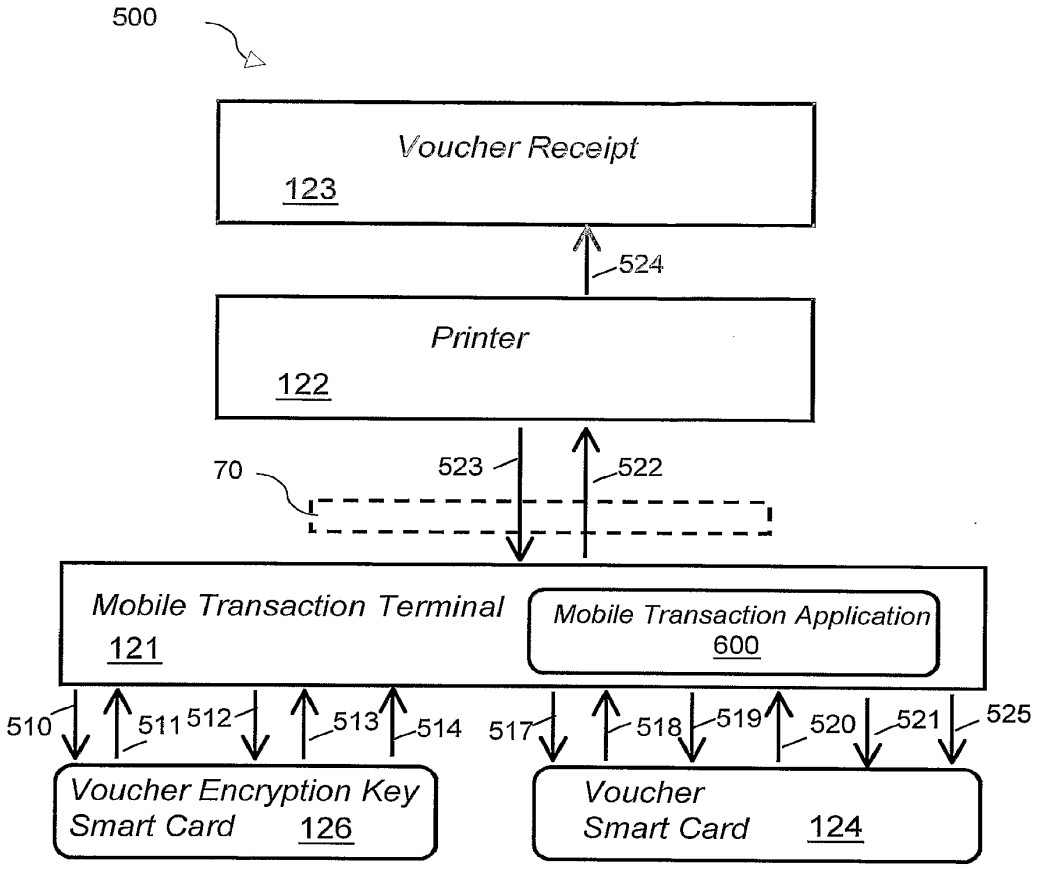

500
Voucher Receipt
123
524
Printer
122
70
523
522
Mobile Transaction Terminal
121
Mobile Transaction Application
600
510
511
512
513
514
517
518
519
520
521
525
Voucher Encryption Key
Smart Card
126
Voucher
Smart Card
124

FIG. 6

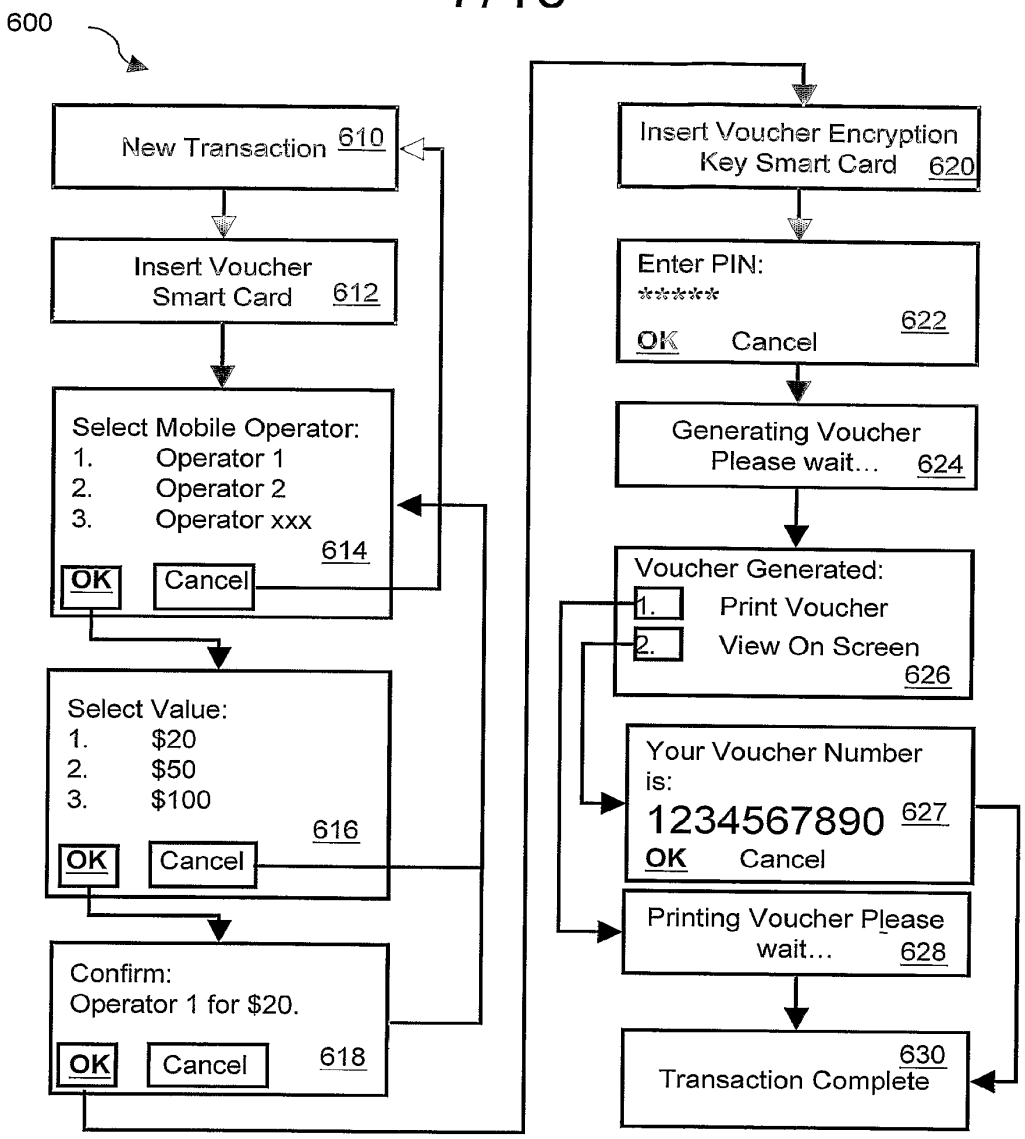

600
New Transaction 610
Insert Voucher Smart Card 612
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
614
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
616
OK
Cancel
Confirm:
Operator 1 for $20.
OK
Cancel
618
Insert Voucher Encryption Key Smart Card 620
Enter PIN:
******
622
OK
Cancel
Generating Voucher Please wait... 624
Voucher Generated:
1. Print Voucher
2. View On Screen
626
Your Voucher Number is:
1234567890 627
OK
Cancel
Printing Voucher Please wait... 628
630
Transaction Complete

FIG. 7

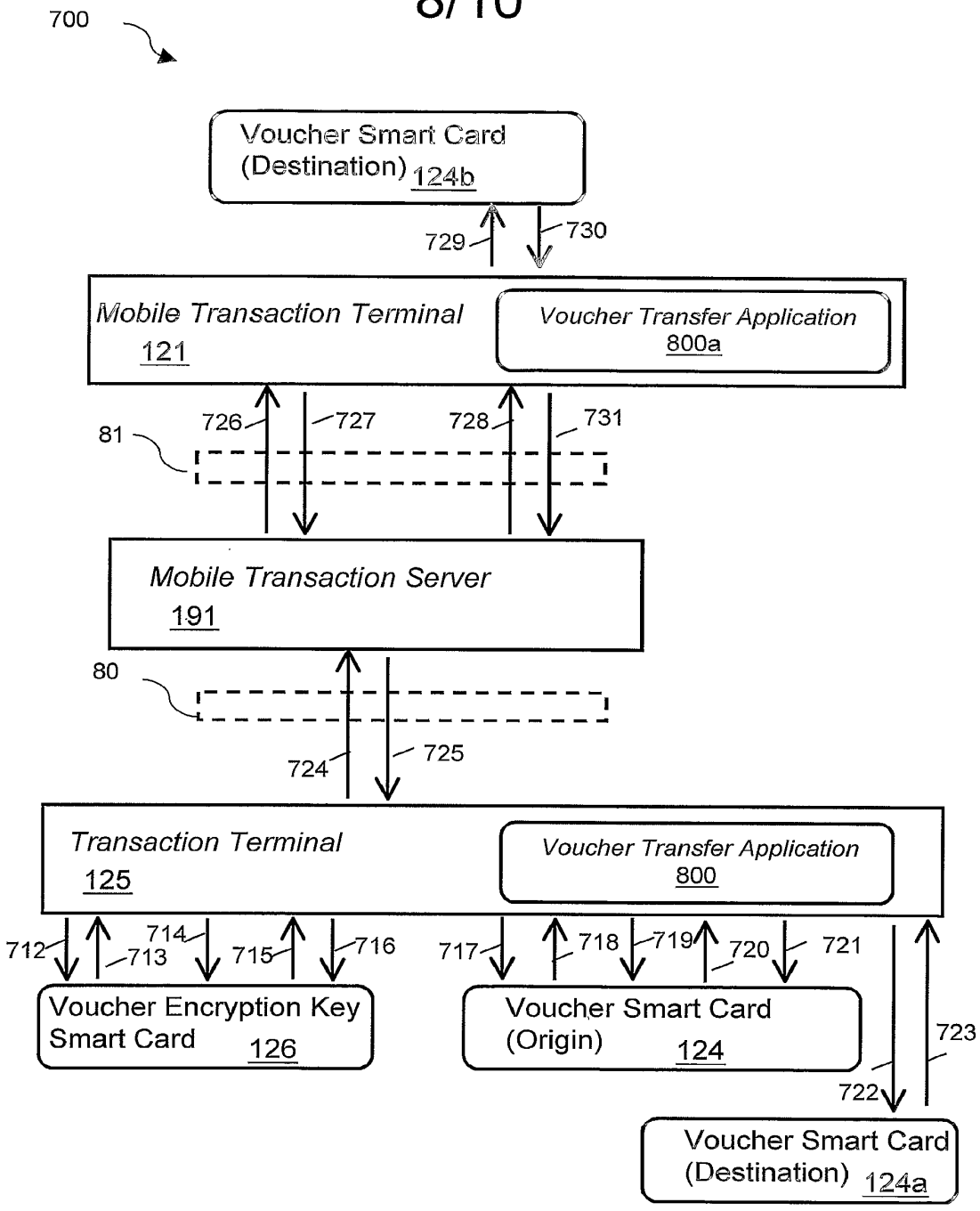

700
Voucher Smart Card (Destination) 124b
729
730
Mobile Transaction Terminal 121
Voucher Transfer Application 800a
81
726
727
728
731
Mobile Transaction Server 191
80
724
725
Transaction Terminal 125
Voucher Transfer Application 800
712
713
714
715
716
717
718
719
720
721
723
722
Voucher Encryption Key Smart Card 126
Voucher Smart Card (Origin) 124
Voucher Smart Card (Destination) 124a

FIG. 8

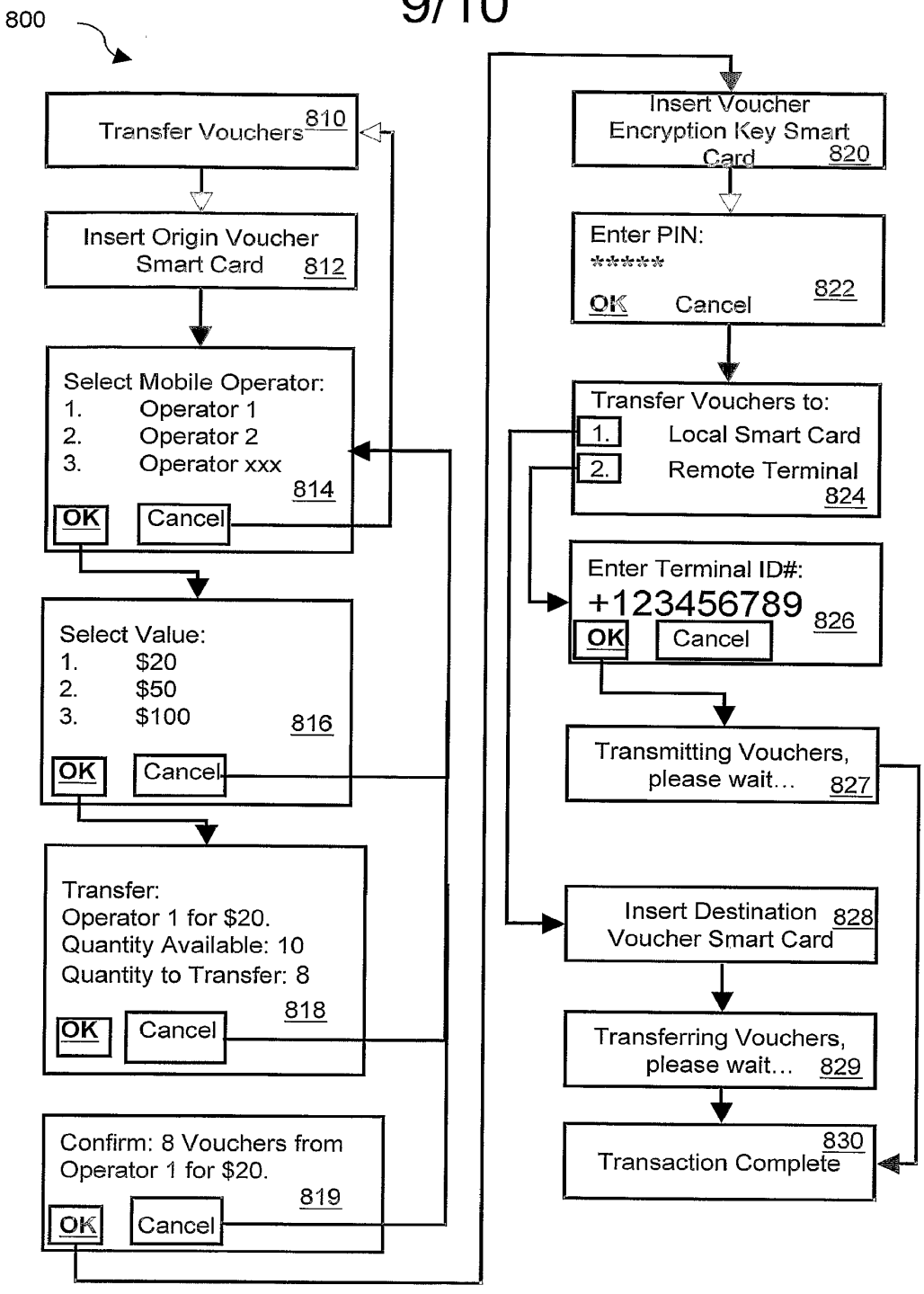

800
Transfer Vouchers 810
Insert Origin Voucher Smart Card 812
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
814
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
816
OK
Cancel
Transfer:
Operator 1 for $20.
Quantity Available: 10
Quantity to Transfer: 8
818
OK
Cancel
Confirm: 8 Vouchers from Operator 1 for $20.
819
OK
Cancel
Insert Voucher Encryption Key Smart Card 820
Enter PIN:
*****
822
OK
Cancel
Transfer Vouchers to:
1. Local Smart Card
2. Remote Terminal
824
Enter Terminal ID#:
+123456789
826
OK
Cancel
Transmitting Vouchers, please wait... 827
Insert Destination Voucher Smart Card 828
Transferring Vouchers, please wait... 829
830
Transaction Complete

FIG.9

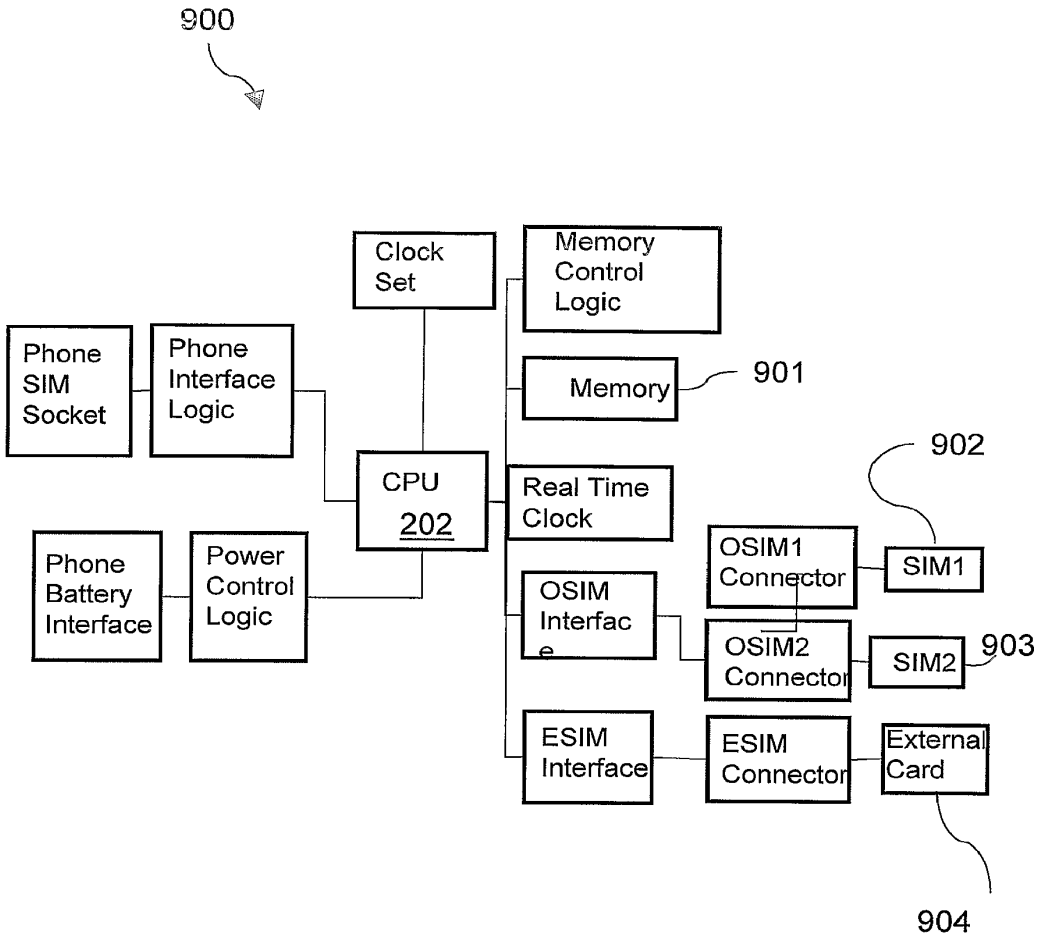

900
Clock Set
Memory Control Logic
Phone SIM Socket
Phone Interface Logic
Memory
901
902
CPU 202
Real Time Clock
Phone Battery Interface
Power Control Logic
OSIM1 Connector
SIM1
OSIM Interfac e
OSIM2 Connector
SIM2
903
ESIM Interface
ESIM Connector
External Card
904

FIG. 10

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 September 2005 (01.09.2005)

PCT

(10) International Publication Number
WO 2005/079254 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/004049

(22) International Filing Date: 10 February 2005 (10.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/544,300	17 February 2004 (17.02.2004)	US
60/549,148	3 March 2004 (03.03.2004)	US
60/575,835	2 June 2004 (02.06.2004)	US
11/045,484	31 January 2005 (31.01.2005)	US

(71) Applicant *(for all designated States except US)*: **FUJITSU LIMITED** [JP/JP]; 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 (JP).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LABROU, Yannis** [GR/US]; 519 West Pratt Street, #410, Baltimore, MD 21201 (US). **JI, Lusheng** [CN/US]; 15 Berry Lane, Randolph, NJ 07869 (US). **AGRE, Jonathan, Russell** [US/US]; 800 Brighton Knolls Drive, Brinklow, MD 20862 (US). **MOLINA TERRIZA, Jesus** [ES/US]; 1000 6th Street, Southwest, #704, Washington, DC 20024 (US). **CHEN, Wei-Lun** [CN/US]; 440 Ridge Road, #4, Greenbelt, MD 20770 (US).

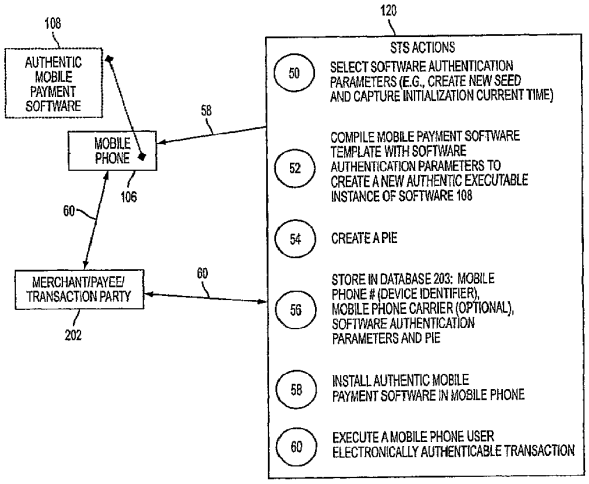
(74) Agent: **SHEIKERZ, Mehdi, D.**; Staas & Halsey LLP, Suite 700, 1201 New York Avenue, Washington, DC 20005 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: WIRELESS WALLET



(57) Abstract: A mobile phone system and method of initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software; providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software; installing, in a mobile phone, the authentic mobile payment software; and inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over the mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol.

WO 2005/079254 A2

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WIRELESS WALLET

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application is related to and is a continuation-in-part of US application no. 10/458,205, filed June 11, 2003, which claims the benefit of US provisional application no. 60/401,807, filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,584 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,569 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002; and also a continuation-in-part of US application no. 10/628,583 filed July 29, 2003, which claims the benefit of US provisional application no. 60/401,807 filed August 8, 2002.

[0002] This application is also related to and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/544,300, Attorney Docket No. 1634.1002P2, entitled A UNIVERSAL PERVASIVE TRANSACTION FRAMEWORK APPLICATION: WIRELESS WALLET ON A MOBILE PHONE, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed February 17, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0003] This application is also related to, and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/549,148, Attorney Docket No. 1634.1002P3, entitled WIRELESS WALLET, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed March 3, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0004] This application is also related to, and also claims the benefit of priority to, Provisional Application U.S. Serial Number 60/575,835, Attorney Docket No. 1634.1002P4, entitled A WIRELESS WALLET FOR PERSON-TO-PERSON TRANSACTIONS, by Yannis Labrou, Jonathan Agre, Lusheng Ji, Jesus Molina Terriza, Wei-lun Chen, and, filed June 2, 2004 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0005] This application is related to Provisional Application U.S. Serial Number 60/401,807, Attorney Docket No. 1634.1002P, filed August 8, 2002 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0006] This application is related to U.S. Serial Number 10/458,205, Attorney Docket No.

1634.1003, entitled SECURITY FRAMEWORK AND PROTOCOL FOR UNIVERSAL PERVASIVE TRANSACTIONS, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed June 11, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0007] This application is related to U.S. Serial Number 10/628,584, Attorney Docket No. 1634.1002, entitled METHODS FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0008] This application is related to U.S. Serial Number 10/628,569, Attorney Docket No. 1634.1004, entitled APPARATUSES FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0009] This application is related to U.S. Serial Number 10/628,583, Attorney Docket No. 1634.1005, entitled FRAMEWORK AND SYSTEM FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0010] The present invention is directed to wireless computing device authenticable transactions, for example, authenticable cashless monetary transactions. For example, a mobile phone wireless wallet.

2. Description of the Related Art

[0011] The future ubiquitous computing environment will consist of mobile users with information computing appliances (mobile devices), such as cellular phones or Personal Digital Assistants (PDA's), that will be wirelessly communicating and interacting with the varied services and devices encountered at any particular moment and place. Many applications that operate in such environments have been proposed from the research and business community, but there has not yet been a strong market pull for any particular one. It is apparent that a crucial enabler for ubiquitous computing to emerge into the marketplace is the ability to safely conduct financial transactions using mobile devices in this form of environment.

[0012] However, mobile devices, and, in particular, mobile phones, can present certain characteristics, such as limited capabilities (computation power, communication bandwidth,

battery capacity, small display, limited keyboard, etc), a typical user who is not technically savvy and cannot be overly burdened with a complex application for executing transactions with other parties, and a wireless transport network that is deemed insecure at the network layer.

[0013] There have been many approaches and solutions proposed for the mobile commerce (m-commerce) problem. A few small manufacturers have offered Wireless Local-Area Network (WLAN)-enabled mobile phones and both MOTOROLA and NOKIA have made announcements of plans to offer such phones in 2004.

[0014] The current m-commerce practice involves Web Store-Front Payment, in which a consumer pays for goods or services offered by a retailer that has Internet presence. For web pages that are specially prepared for mobile devices, such as those that are WAP-enabled, one could use the mobile device to make a purchase as it is normally done in e-commerce transactions using a web browser on a personal computer. But, since payment typically requires logging in and typing a username and password, this approach is impractical and inefficient on a mobile device, even if the transaction uses Wireless Application Protocol (WAP) and has occurred through a secured network link such as through https or Secure Socket Layer (SSL). In many current web browsing applications, the consumer can pre-register one or more financial accounts with a merchant to save time and avoid repeatedly entering ones financial information, but this approach requires a consumer to register multiple user account information with multiple merchants. Further, in case of a physical point-of-sale (POS) case it is too complex to deploy from a business point of view because it frequently involves integration with the back-end store systems and some form of binding between the payer and the physical goods purchased.

[0015] From a data security perspective, existing m-commerce data security solutions rely on Public Key Infrastructure (PKI) technologies. However, PKI solutions suffer from poor computational performance in mobile device environments and complexity of the user experience. There are many different ways PKI can be used for mobile payments. One proposed PKI-based solution for mobile payments is by MET LIMITED, which is discussed at [www.mobiletransaction.org, retrieved on January 5, 2005]. Under existing m-commerce security solutions, a user signs a transaction (a purchase order) with a certificate that authenticates the identity of the user (it is unclear whether each user has a single such certificate or a variety of them, each for every eligible account). For example, handling of multiple security certificates from many vendors is confusing, at best, and can be dangerous if left up to the user. Since these certificates are stored on the mobile device, the certificate store needs to be protected and "unlocked" on a per use basis. If the certificate storage is

implemented in software the key used to unlock the storage should be of sufficient length to protect this storage, or it can be instead implemented in hardware, which in case of a mobile phone would require the phone to be designed for this purpose. Such an approach requires an infrastructure for dissemination of certificates (including revocation), possibly specialized mobile phones and possibly some basic understanding by the user of certificates and their usage.

SUMMARY OF THE INVENTION

[0016] The embodiments described herein relate to wireless mobile computing device user electronically authenticable transactions, for example, mobile phone user authenticable cashless monetary transactions. For example, a user mobile phone wireless wallet.

[0017] A mobile phone system and method of initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software; providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software; installing, in a mobile phone, the authentic mobile payment software; and inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed, secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol.

[0018] The above as well as additional aspects and advantages will be set forth in part in the description which follows and, in part, will be obvious from the description, or may be learned by practice of the described embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] These together with other aspects and advantages which will be subsequently apparent, reside in the details of construction and operation as more fully hereinafter described and claimed, reference being had to the accompanying drawings forming a part hereof, wherein like numerals refer to like parts throughout.

FIG. 1A is a flow chart of activating a mobile phone cashless monetary transaction capability, according to an embodiment of the present invention.

FIG. 1B is a flow chart of activating a mobile phone cashless monetary transaction capability, according to another embodiment of the present invention.

FIG. 1C is a diagram of mobile phone display screen user interface images to activate a mobile phone cashless monetary transaction, according to an embodiment of the

present invention.

FIG. 2 is a functional block diagram of Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) system architecture to execute a mobile device cashless monetary transaction, according to an embodiment of the present invention.

FIG. 3 is functional block diagram of a UPTF based system architecture to execute a mobile phone cashless monetary transaction with a physical point of sale (POS), according to an embodiment of the present invention.

FIG. 4 is a diagram of UPTF cashless monetary transaction messages based upon Secure Agreement Submission (SAS) protocol to execute a mobile phone cashless monetary transaction, according to an embodiment of the present invention.

FIG. 5 is a flow chart of a UPTF based mobile phone cashless monetary transaction with a merchant, according to an embodiment of the present invention.

FIG. 6 is a flow chart of a UPTF based mobile phone cashless monetary transaction to purchase a movie ticket, according to an embodiment of the present invention.

FIGS. 7A-B are mobile phone display screen user interface images to execute mobile phone cashless monetary transaction to purchase a movie ticket, and to obtain, store, and retrieve a transaction receipt, according to an embodiment of the present invention.

FIG. 8 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment transaction, according to an embodiment of the present invention.

FIG. 9 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment request transaction, according to an embodiment of the present invention.

FIG. 10 is overall mobile phone display screen user interface images and possible workflows available to an operator of a wireless wallet on a mobile phone to execute peer-to-peer cashless monetary transactions, according to an embodiment of the present invention.

FIGS. 11-12 are diagrams of mobile phone cashless monetary transaction message formats to execute various mobile phone person-to-person cashless monetary transactions, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Reference will now be made in detail to the present embodiments of the present invention, examples of which are illustrated in the accompanying drawings. The embodiments are described below to explain the present invention by referring to the figures.

[0021] Generally, there can be three classes of mobile commerce transactions, as follows:

[0022] 1. Person-to-person payments: A consumer can directly make an agreed upon payment to another consumer using their mobile devices.

[0023] 2. Web Store-Front Payment: A consumer pays for goods or services offered by a retailer that has an Internet presence. A user browses the retailer's web pages using a mobile device to identify the good or service to be purchased and then conducts payment. Examples of this case would be paying for a book or purchasing movie tickets through a web service.

[0024] 3. Physical Point-of-Sale (POS) purchase: A consumer pays a retailer at a check-out station using the mobile device, such as when making a payment at a "brick and mortar" store or restaurant.

[0025] The boundaries between these categories are malleable and their common properties can be exploited using the transaction agreement point of view. The embodiment(s) described herein accommodates these and/or other mobile commerce transactions.

[0026] In the described embodiments herein, a mobile device is any wireless handheld, or hand size, electronic computing device, including, without limitation, a mobile phone. The embodiment(s) described herein relate to wireless mobile computing device user electronically authenticable transactions based upon Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol, such as (without limitation) mobile phone user authenticable transactions that may or may not result in a financial settlement, and/or mobile phone user authenticable cashless financial/monetary transactions. For example, a user authenticable mobile phone wireless wallet. More particularly, according to an aspect of the embodiment(s) described herein, a wireless mobile computing device provides user electronically authenticable transactions according to time and software dependent secured (e.g., encrypted), matched (verified against each other), and transaction party anonymous, transaction view(s) of one or more parties (i.e., in a typical embodiment paired and/or more than two transaction views).

[0027] FIG. 1A is a flow chart of activating a mobile phone cashless monetary transaction capability, according to an embodiment of the present invention. A computer system and method for a wireless mobile computing device user electronically authenticable transactions (i.e., electronic authentication of a user and/or the user's transaction) comprises, at operations 50 and 52, initializing, at a secure transaction server (STS) 120, a mobile payment software template with software authentication parameter(s), as an authentic mobile payment software 108. At operations 54 and 56, correlating, at the STS

120, a personal identification entry (PIE) and an identifier of a mobile phone 106 with the authentic mobile payment software 108. At operation 58, installing, in the mobile phone 106, the authentic mobile payment software 108. At operation 60, executing, at the mobile phone 106, the installed authentic mobile payment software 108 using the PIE to execute a mobile phone authenticable cashless monetary transaction as a mobile phone wireless wallet of a user of the mobile phone 106. More particularly, at operation 60, inputting by a user the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter, a transformed secure authenticable mobile phone cashless monetary transaction. According to an aspect of the embodiment described herein, at operation 50, one or more software authentication parameters are selected, which can be (without limitation) creation of a new seed, such as a new random seed number, and an initialization time. At operation 56, the STS 120 stores in a database 203, a unique identifier (referred to as Device ID, or DID) for the mobile phone 106, which can, for example, be a mobile phone number of the mobile phone 106 or some randomly generated globally unique identifier (GUID), a mobile phone carrier (as the case may be), the software authentication parameter(s) selected at operation 50, and the generated PIE. According to an aspect of the described embodiment, a mobile phone number can also be used as a device identifier for the mobile phone 106. The unique identifier (device ID (DID)) of the mobile phone 106 is used by the STS 120 to correlate a transaction message with authentic mobile phone payment software 108; to correlate the DID with the software authentication parameter(s) and the PIE stored at the STS 120 so that the STS 120 can generate a key that corresponds to a device 106 having the DID. The mobile phone number can be used to communicate (e.g., notifications, etc.) with the mobile phone 106 (e.g., Short Message Service (SMS) and/or Multimedia Message Service (MMS)). The mobile phone 106 can be an Internet enabled, according to known techniques, mobile phone. The PIE is described in more detail further below. The mobile phone authenticable cashless monetary transaction is performed according to an agreement view(s) protocol known as Universal Pervasive Transaction Framework (UPTF) (described in more detail below) and secured (e.g., encrypted) according to a protocol known as Secure Agreement Submission (SAS) (described in more detail below). According to an aspect of the embodiment(s) described herein, a transaction message is bound to a unique combination of a user and a device (e.g., mobile phone wireless wallet 106), the binding to the user is via the PIE and the binding to the device 106 is via the software authentication parameter(s) of the authentic mobile payment software 108. In particular, a transaction is an SAS based encrypted message and the encrypted message can be traced back to a combination of the user and the device 106 through the PIE and the software authentication parameter(s) of the authentic mobile payment software

108.

[0028] FIG. 1B is a flow chart of activating a mobile phone cashless monetary transaction capability, according to another embodiment of the present invention. In FIG. 1B, a computer system and method comprises, at operation 100, providing to a user a mobile phone cashless monetary transaction activation link at a computing device 102 (sign-up application 102), at operation 104, registering a phone number of a mobile phone 106 of the user via the activation link, at operation 105, associating a mobile payment software 108 with software authentication parameters, as an authentic mobile payment software 108, and, at operation 110, providing a correlation between a personal identification entry (PIE) and the authentic mobile payment software 108, at the STS 120. At operation 112, a mobile phone download link to the mobile payment software 108 is transmitted to the mobile phone 106, using the registered phone number of the mobile phone 106. At operation 114, the mobile payment software 108 is downloaded to the mobile phone 106 via the download link. At operation 116, the user can activate the downloaded mobile payment software 108 using an optional activation code. After installation of the authentic mobile payment software 108, as a user mobile phone wireless wallet 106 of the mobile phone user (i.e., a mobile phone wireless wallet application 108), the user can execute a mobile phone user electronically authenticable cashless monetary transaction using the user mobile phone wireless wallet 106.

[0029] The mobile payment software 108 is implemented according to an application platform of the mobile phone 106. For example, the mobile payment software 108 can be implemented according to Java 2 Platform Micro Edition (J2ME). According to an aspect of the embodiment described herein, at operation 112, the mobile payment software downloaded link is transmitted to the mobile phone 106 using short message service (SMS) and/or multimedia message service (MMS).

[0030] In FIG. 1B, after operation 116, a mobile phone cashless monetary transaction may be performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol. The UPTF SAS protocol is discussed in related commonly assigned pending US patent application nos. 10/458,205, filed June 11, 2003; 10/628,584, filed July 29, 2003; 10/628,569, filed July 29, 2003; and 10/628,583, filed July 29, 2003, owned by FUJITSU LIMITED assignee of the present Application, the entire disclosures of all of which are hereby incorporated herein by reference.

[0031] In FIG. 1B, at operation 105, the associating of the mobile payment software 108 with the software authentication parameters comprises generating a UPTF random number identifier by a provider 122 of the mobile phone cashless monetary transaction activation, so

that the UPTF random number can be associated with the user and transmitting the UPTF random number identifier and the registered phone number of the mobile phone 106 to a secure transaction server (STS) 120. For example, at operation 105, in case the provider 122 is a payment service 122 at which a transaction party (a user) registers financial account information, the payment service 122 can assign a UPTF random number identifier (abstracted identifier) 123 to identify the user when communicating with the STS 120. Accordingly, the STS 120 can communicate with the provider 122 to execute a UPTF based transaction based upon the provider 122 UPTF random number and without knowledge of actual transaction party account information. Further, operation 110, comprises generating, by the STS 120, an executable mobile payment software including the initialization parameters, as the authentic mobile payment software, and generating the PIE that is correlated in the STS with the authentic mobile payment software 108. At operation 112, the transmitting of the mobile payment software download link comprises transmitting, by the STS 120, via short message service (SMS) the mobile payment software 108 download link to the mobile phone 106 of the user; and providing, by the STS 120, the PIE to the user. The described embodiment is not limited to the above-described authentic mobile payment software 108 generation, activation, and installation, and, at operation 58, an authentic mobile payment software 108 can be installed or provided for a mobile phone 106 via mobile phone removable/installable (e.g., smart card) and/or embedded computer readable media, embedded in a mobile phone computing processor, via an emailed download link, emailed attachment, etc.

[0032] FIG. 1C is a diagram of mobile phone display screen user interface images to activate a mobile phone cashless monetary transaction, according to an embodiment of the present invention. User interface screen image 150 is displayed at operation 112, when the mobile phone 106 receives an SMS message from the STS 120 on behalf of the provider 122. User interface screen image 152 displays the received SMS message directing the mobile phone user to go to an Internet address to download the authentic wireless wallet software 108. The user interface screen image 154 is displayed after operation 114, when downloading of the authentic wireless wallet software 108 to the mobile phone 106 is completed. The user interface screen image 156 is displayed when installing the authentic wireless wallet software 108. The user interface screen image 158 is displayed at operation 116, when an optional activation code for the authentic wireless wallet software 108 has been provided to be input at the mobile phone 106. After input of the activation code via the user interface screen image 158, the user interface screen image 160 is displayed, confirming to the user that the authentic wireless wallet software 108 has been activated and ready for executing mobile phone user electronically authenticable cashless monetary

transactions.

[0033] According to an aspect of the described embodiment herein, at operation 100, a provider 122, such as an online payment system/service, a merchant/service provider, a financial institution, etc., provides the mobile phone cashless monetary transaction activation link to a member of the provider 122 as the user. In case of an online payment system 122, the described embodiment provides member-to-member mobile phone cashless monetary transactions using the user mobile phone wireless wallet 108.

[0034] According to an aspect of the described embodiment herein, at operation 110, the STS 120 sends the PIE to the provider 122, and, at operation 111, the provider 122 receives the PIE and displays the PIE to the user at the computer 102. At operation 111, for additional security, the PIE might only be an image so that the provider 122 does not know the PIE, thereby allowing for anonymity of the transaction parties. The PIE can be delivered according to other secured ways, such as mail, email, a customer service representative, etc.

[0035] Therefore, with reference to FIGS. 1A and 1B, in an unlimiting example, the wireless wallet application 108 is implemented as a J2ME application than can be downloaded and executed on the mobile phone 106 and enables users to make purchases and payments leveraging Universal Pervasive Transaction Framework (UPTF). Currently, many mobile phones offered by carriers in the US are J2ME enabled and web-enabled, such that the wide-spread availability of J2ME on mobile phones enables new business models with respect to the delivery of content and services to mobile users. With J2ME, anyone can develop downloadable J2ME applications for custom content or service delivery to the mobile. This is the case of the wireless wallet application 108, which allows offering the service of secure payments using mobile phones 106.

[0036] The J2ME wireless wallet application is a relatively small application (typically according to the present invention less than 90 Kbytes) which combines the functionality of a web browser (for example, a cHTML web browser) and that of the purchasing application that implements the UPTF SAS framework and security protocol. It allows mobile users to enable or disable the payment functionality and to store receipts of purchase. The wireless wallet method can be offered by any retailer or payment service in order for consumers to make payments with their mobile phone. It is a completely software solution to the problem of secure payments using a mobile device. If the provider of the wireless wallet is a web store-front retailer, such as a movie ticket provider, the wireless wallet application 108 can be used to make payments with any of the accounts registered with the retailer. If the provider is an Online Payment Service, the wireless wallet software 108 can be used to make

payments to other online payment service users (person-to-person) or to "brick and mortar" retailers that accept payment with this payment service or a central service/system that can interface a plurality of payment services. In the latter case, the merchant can use a merchant's version of the wireless wallet client 108 to specify transaction information, such as the payment amount. The issue of identifying what is being paid for by the consumer via a mobile phone 106 is addressed by having the consumer enter a receipt number (e.g., as printed in the receipt of the restaurant where the meal is paid for) and/or a merchant identifier (e.g., a phone number of the merchant, including merchant POS identifier, etc.) on their wireless wallet application 108 to interface with the merchant retail application software; the goal being to bind a virtual shopping cart to a specific consumer.

[0037] A more detailed mobile payment software 108 download and activation is described as follows:

[0038] 1. After a user logs into a Provider's 122 web site using a computer device, such as personal computer 102, the option of using one's mobile phone for payments is presented and the user is re-directed to a page where one is asked for a phone number of the mobile phone to be used for mobile phone cashless money payments.

[0039] 2. The Provider 122 generates a UPTF_ID (random number) for the already captured username and password (operation 105) and sends to the STS 120 the UPTF_ID and mobile number. Therefore, in this example, the Provider 122 does not have to share with the operator of the STS 120 real account information of the user, but the provider 122 and the STS 120 relate transactions to a user based upon a random identifier generated by the provider 122.

[0040] 3. The STS 120 then creates a new wireless wallet executable 108 (with "fresh" initialization parameters per the UPTF requirements), a link to download this executable, an optional activation code, and a personal identification entry (PIE), all of which are correlated at and maintained by the STS 120 (operations 50-56 and 110). The STS 120 can send the PIE to the Provider 122.

[0041] 4. If the STS 120 sends the PIE to the Provider 122, the PIE is received by the provider 122 and displayed to the user (operation 111). Optionally, the STS 120 can provide an activation code to the user via SMS (e.g., at operation 116) or via the provider 122 (e.g., at operation 111). Alternatively, the PIE and the activation code (as the case may be) can be communicated to the user through channels other than the provider 122 or SMS, for example, via mail, email, etc. Typically in the present invention, the activation code is a number (for easier user entry) and used as a one time password that encrypts the UPTF-

related initialization parameters of the downloaded software 108, so that if a third party attacker intercepts the software while in transit, the attacker cannot have access to the device-specific initialization parameters.

[0042] 5. The STS sends a Short Message Service (SMS) message to the previously entered mobile's phone number with the download link (operation 112).

[0043] 6. The mobile user downloads the wireless wallet software 108 (e.g., at operation 114, the link can be easily followed directly from the SMS text itself) and subsequently uses the wireless wallet software 108 (operation 116). An initial activation can involve using the activation code. Otherwise, at operation 116, the user can subsequently use the wireless wallet software 108 to execute a mobile phone cashless monetary transaction by using only the PIE.

[0044] After operation 114 (after downloading wireless wallet application 108 into the mobile phone 106), the wireless wallet 108 is ready for use; purchases and/or financial transactions can be paid for with any of the accounts registered with the wireless wallet provider 122. This scheme for distributing the software ensures a secure distribution of the software, on request, and a safe dissemination of the PIE. A mobile phone wireless wallet software 108 distribution model has been implemented for downloading and installing a J2ME executable on the mobile phone 106. Operation of the software 108 is very easy and transaction time largely depends on the speed of the mobile phone carrier's network. Based on tests, a mobile phone cashless monetary transaction time can vary between 30 and 45 seconds, the differences due to a mobile carrier's network-related delays. The traffic generated by the mobile payment software application 108 (following the determination of what is purchased) is less than 1KByte (send/receive) for each transaction, as each mobile phone cashless monetary transaction message can be smaller than 256 bytes. In an unlimiting example, communication between the mobile phone 106 and the STS 120 during payment was routed either through a provider 122 or directly to the STS 120 (depending on the type of financial transaction and as will be described in more detail below) and was carried over Internet Hypertext Transfer Protocol (HTTP) on a mobile phone communication network. More particularly, because the UPTF SAS security is session-less based upon message view (as described in more detail below) encryption (i.e., not based upon communication session security), such as secure socket layer (SSL), secured transaction processing efficiency by the mobile phone 106 is substantially improved.

[0045] FIG. 2 is a functional block diagram of Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) system architecture to execute a mobile device cashless monetary transaction, according to an embodiment of the present

invention. In FIG. 2, colors are used to highlight features/concepts described herein. The Universal Pervasive Transaction Framework (UPTF) defines a system architecture based upon independent and anonymous transaction agreement views and a communication security protocol called the Secure Agreement Submission (SAS) protocol to transmit the views. Essentially the UPTF offers a vessel, which is able to securely carry the individual views of a transaction agreement from each party involved in the transaction to a trusted third party for verification, using a communication network which may consist of insecure segments such as wireless LANs or cellular links. When used for financial applications, such as the electronic wireless wallet, the transaction parties are payer 200 and a payee 202, for example, a customer payer 200 and a merchant payee 202, and a typical example of an "agreement" may read: "Party A will pay Party B $X for item Y."

[0046] The UPTF SAS protocol encrypts/decrypts a transaction message using a symmetric, secret-key approach where the secret key is producible only by an individual party's device 106 and a trusted third party (e.g., implemented as STS 120) and without transmission of the secret key among the parties. In other words, the UPTF SAS provides an implicit user authentication, because decryption by a trusted third party, such as STS 120, of a sending party's encrypted message, authenticates the sending party. The SAS insures that the authenticity of the parties is verified and during delivery, the privacy of the information is preserved (transaction party anonymity), even when the parties distrust each other and the messages from one party may be forwarded by the other to the third party verification. The UPTF also provides the mechanism for the trusted third party to verify that the independent views of the agreement are consistent with each other.

[0047] After the agreement data is extracted from the transaction views received from the parties and the data is verified by the trusted third party, further actions may need to be taken to actually execute the agreement. This is realized by the trusted third party interacting with the financial institutions associated with the payer 200 and the payee 202 to cause the transfer of the specified funds between the customer payer 200 and the merchant payee 202.

[0048] The wireless wallet UPTF system architecture is shown in FIG. 2 and comprises: a Payer 200 operating a UPTF device (called a UPTD), such as a mobile phone 106 loaded with a mobile phone wireless wallet 108, a Payee 202 operating another UPTF device, a Secure Transaction Server (STS) 120, a number of financial institutions 204, and several communication channels among them. For example, the payer 200 operates the mobile phone wireless wallet 106 to interact with the Payee 202 to determine the details of a purchase transaction and executes the UPTF protocol and its corresponding security

operations SAS. The mobile phone wireless wallet 106 can support wireless communication capability necessary for discovering/interfacing with the payees 202 via service spots of the payees 202 (a place where a signal can exist to connect to the mobile phone wireless wallet 106). The wireless communication capability of the mobile phone wireless wallet 106 to communicate with a service spot payee 202 and/or an STS 120 can be wireless local area network (WLAN) and/or mobile phone communication (cellular) network. The mobile phone wireless wallet 106 can also have a user interface for interacting with the payee 202 through some common application and to the STS 120 as needed. The Payee 202 can also operate a UPTD, such as a merchant transaction server (MTS) 302 that implements a retail application, and is responsible for interacting with the payer 200, executing the UPTF protocol and its corresponding security operations and interacting with the STS 120. In FIG. 1B, in case the provider 122 is an online payment system, the provider 122 would correspond to the financial institutions 204 of FIG. 2, which allows any type of UPTD person-to-person cashless monetary transactions via Channels A, B, and C as logical communication channels. Of course, the STS 120 and the financial institutions 204 might be implemented by a single entity or separate entities, as the case may be.

[0049] According to an aspect of the embodiment described herein, the STS 120 is a backend verification server on which both the payer 200 and the payee 202 have registered and provided identifying account information that is maintained in a secure STS database 203. The secret information used for encrypting the messages to/from each payer 200 and payee 202 are also stored in this DB 203. The STS 120 receives independently generated UPTF SAS transaction views (described in more detail further below) from both the payer 200 and the payee 202 regarding a financial transaction conducted between them. The STS 120 is able to decode both of the views using information from UPTF SAS cashless monetary transaction messages and the information stored in the STS 120 database 203. Following successful decoding, the STS 120 verifies that the view messages are original, authentic, involve the intended payer 200 and payee 202 and that the information fields in the agreement views are consistent with each other. The STS 120 will maintain a log of messaging activity for non-repudiation purposes.

[0050] In FIG 2, a generic set of communication channels are explicitly indicated. The indicated communication channels reflect anonymity of the transaction party communications (anonymous transaction party communication channels) according to the UPTF. Channel A (Ch A) logically represents the link between the payer 200 and the payee 202. This link is used to negotiate the details of a cashless payment transaction. This aspect is application dependent and is not considered to be part of the UPTF framework. Ch

A may or may not exist, and if it exists it can be a wireless channel, for example, in case of a WLAN enabled mobile phone 106, and/or channel A can be oral communication between the payer 200 and payee 202 in case of a non-WLAN mobile phone 106 used in a point of sale financial transaction. Channels B and C, are example logical links among the Payer 200, the Payee 202, and the STS 120. In case of a mobile phone wireless wallet 106, Channels B and C are mobile phone communication networks that can carry Internet traffic. In most situations these are not direct links, but involve communicating through the mobile communications network and/or the Internet. In general, these are insecure channels. Channel D, from the STS 120 to the Financial Institutions 204 is a different type of channel and is assumed to be a highly secure communication path. In addition, STS 120 itself is assumed to be housed in a protected facility so that its database 203 is physically secure and inaccessible from the network.

[0051] The mobile phone wireless wallet 106 operations involved in an example transaction with reference to FIG. 2 is described. The payer (operator) 200 initiates the SAS protocol through an explicit action, enters the PIE generated in operation 110 by the STS 120. This allows the payer 200 to generate a view of the transaction and to encrypt this with its private key based upon the PIE and the software authentication parameter(s) and then to send the encrypted view as a message to the STS 120. Similarly, the payee (operator) 202 enters its PIE that is also generated in operation 110 by the STS 120 and generates it's own view of the transaction, encrypts the view with its private key based upon the PIE and the software authentication parameter(s) and then sends its view to the STS 120. The STS 120 receives both encrypted views and verifies the views, through a successful view decryption (i.e., a successful view decryption authenticates a user) and a successful comparison of two or more views (as the case may be) (i.e., a successful comparison of transaction party views authenticates a transaction). The STS 120 then uses the secure back channels D to interact with the financial institutions 204 of the payer 200 and the payee 202 for transferring the funds. The STS 120 sends receipts (or failure notices) back to the payer 200 and the payee 202 to complete the transaction. The response messages are also encrypted by the STS 120 for each intended destination.

[0052] Other examples described herein are particular instances of the FIG. 2 UPTF system architecture. In particular, the physical POS deployment represents a common variation of this scheme. For this situation, the Payer 200 is a customer device, such as the mobile phone 106 that executes the wireless wallet application 108, the Payee 202 is the merchant operated device. The merchant operated device is located at a fixed site and can be a more powerful computer and provide additional network services, such as an Internet

connection. A direct payer 200 to STS 120 Ch B is not used, but rather the Payer 200 UPTF cashless monetary transaction messages are forwarded to the STS 120 through the merchant 202. In this case, channels A and B would be a mobile communication channel between the payer 200 and the merchant server 302 to bind the mobile phone user with transaction information of the merchant, such as the merchant products/services available for purchase and to forward, by the merchant server 302 to the STS 120, the payer 200 UPTF transaction messages (see FIGS. 3, 5 and 6). The properties of the protocol prevent the merchant from gathering personal information from the customer 200. Further details of the encryption procedures as part of the SAS are described further below.

[0053] Therefore, the mobile phone 106 wireless wallet application 108 is based on a general framework, called the Universal Pervasive Transaction Framework (UPTF), a generic architecture and a new security protocol for conducting secure multi-party agreements, using mobile devices over a wireless transport network. The framework is designed to address several key aspects specific to the envisioned pervasive environments.

[0054] FIG. 3 is functional block diagram of a UPTF based system architecture to execute a mobile phone cashless monetary transaction , according to an embodiment of the present invention. A universal pervasive transactions device (UPTD) is a wireless mobile computing device, such as mobile phones 106a-n, based upon the UPTF SAS to implement a wireless wallet by installing in the mobile phones 106a-n corresponding authentic mobile payment software 108a-n. A computer system and method of binding the mobile payment software 108a with transaction information of a transaction party (e.g., merchant online retail application 302); inputting the PIE by the user at the mobile phone 106a of the user; executing the authentic mobile payment software 108a and presenting, by the STS at the mobile phone 106a, a selectable list of abstracted relationship identifiers (identifiers that are a level removed from actual identifiers), corresponding to the registered financial entities of the user, that are correlated with the authentic mobile payment software 108a; and executing the mobile phone cashless monetary transaction with the transaction party 302 using the PIE and the software authentication parameter and according to UPTF transaction messages comprising an identifier of the mobile phone 106a, an identifier of the transaction party 302, and an identifier of the transaction, thereby providing the mobile phone wireless wallet based upon a combination of the authentic mobile payment software 108a at the mobile phone 106a and the STS 120 correlations of the authentic mobile payment software 108a with the PIE, the software authentication parameter, and the financial entities of the user, and independent, anonymous exchange of the UPTF transaction messages between the user, the transaction party and the STS. As described in more detail below, the authentic mobile

payment software 108 and the STS 120 correlations result in generation of a security tool (e.g., an encryption key) to secure (e.g., encrypt) messages, and, thus, successfully decrypting each message authenticates a sender, and, in case of UPTF transaction messages, by decrypting and matching UPTF transaction views of one or more transacting parties authenticates the transaction.

[0055] A UPTD wireless wallet can be a WLAN enabled wallet-sized computing device, including a WLAN enabled mobile phone, able to detect UPTF-enabled physical points of sale (POS), to wirelessly connect to the POS using a wireless local area network/short range radio technology (e.g., 802.11, BLUETOOTH, Infrared, etc.), and to allow their owners to make purchases and or payments with the UPTD wireless wallet. A UPTD wireless wallet can also be a mobile phone without WLAN capability. UPTF authenticable transactions using a UPTD that is a WLAN enabled mobile phone is described in, and can also be understood, for example, by referring to, the pending US patent application no. 10/628,583 (attorney docket no. 1634.1002) filed July 29, 2003 and owned by FUJITSU LIMITED assignee of the present patent application, which is incorporated herein by reference. In a typical embodiment described herein, the UPTD wireless wallet is an Internet and/or web capable/enabled mobile phone 106 (hereinafter referred to as a mobile phone 106 or as a mobile phone wireless wallet 106). For example, a mobile phone wireless wallet 106 could be used to place an order at a restaurant and subsequently make payment, as follows: (1) the user consumer 200, through activating a UPTD mobile phone wireless wallet software 108 function, according to the processes of FIG. 1A, interfaces over a mobile phone communication network 317 with a service spot merchant 202 (which, for example, could be a retail application server 302 on Internet 310 for a movie theater ticket, a gas station, etc., a point of sale 315 at a physical location of the merchant 202) - the retail application 302 implements a virtual store front (for ordering goods or retrieving the payment amount and is accessible through a web server) and implements the UPTF-related functions for effecting mobile phone cashless purchasing; (2) the mobile phone wireless wallet 106 displays a listing of the available merchant 202 offered services (via Channel A between the mobile phone wireless wallet 106 and the retail application 302 in FIGS. 2 and 3); (3) the consumer 200 selects the service (e.g., ordering a meal, or payment at checkout station) with a simple keypad input at the mobile phone wireless wallet 106; (4) once a purchase amount is determined, the consumer 200 presses a designated payment button on the mobile phone wireless wallet 106, which begins the payment stage and results in retrieval of a purchase order (i.e., the agreement) from the merchant 202; following a visual inspection by the consumer 200, the consumer 200 is requested to input the consumer's security PIE (also optionally selecting which financial entity account to use for payment); (5) the consumer 200

receives on the mobile phone wireless wallet 106 a confirmation and a receipt, if the transaction was successful (the service spot merchant 202 also receives a notification of the successful transaction).

[0056] It is important that the payment stage (5) is explicitly initiated by the consumer 200, so that the consumer cannot be spoofed into typing a PIN into an attacker-served page. In a typical implementation of the embodiment described herein, pressing the payment button results in termination of a browsing application (e.g., an execution thread) executed at the mobile phone 106 and the launching of new application (e.g., another execution thread) for user entry (albeit transparent to the user). As long as the user never entered a PIE without first pressing a payment button, hijacking of the PIE can be prevented.

[0057] The retail application 302 implements a virtual store front (for ordering goods or retrieving the payment amount and is accessible through the web server) and the UPTF-related functions for effecting purchasing.

[0058] The mobile phone wireless wallet 106 can deliver a user experience to execute UPTF SAS based cashless monetary transactions in a fast and intuitive manner. The mobile phone wireless wallet software 108 delivers an implicit localization by allowing interfacing at any location (location independent) to merchants 202. The speed and its simple and unified interface are effective and with some practice, performing a transaction could be accomplished in seconds (e.g., 30 seconds, or less than 12 seconds in case of a WLAN mobile phone wireless wallet 106); which can be less than a typical cash or card transaction involving getting change or physical paper receipts. A consumer 200 could purchase (or be offered) a mobile phone wireless wallet 106, for example, on-line via the sign up application computer 102. In other words, the consumer 200 would obtain a PIE as well as obtain (download) a wireless wallet software 108 for a mobile phone to execute mobile phone UPTF SAS based transactions. Merchants 202 would provide UPTF SAS functions in retail and purchasing applications 302, 315.

[0059] FIG. 4 is a diagram of UPTF cashless monetary transaction messages based upon Secure Agreement Submission (SAS) protocol to execute a mobile phone cashless monetary transaction, according to an embodiment of the present invention. In FIG. 4, colors are used to highlight features/concepts described herein. The SAS protocol is used for encrypting and submitting views of desired UPTF based cashless financial transactions. The message structure and encryption mechanism of SAS are designed to provide many of the desired security properties in an insecure pervasive communication environment envisioned for wireless purchasing, such as:

[0060] o Authentication: the agreement parties and the verification party are authenticated to each other, as is the integrity of the agreement group;

[0061] o Anonymity: agreement parties may remain anonymous to each other and personal and/or other account related information is not revealed to the other party;

[0062] o Protection of the agreement content: the agreement is kept private, it is tamper-resistant, non-replayable, and strong non-repudiation proper-ties are provided. In particular, a continuously changing, time dependent, device specific key is used to encrypt the views.

[0063] The underlying SAS algorithms are well-suited for a system using low-cost user devices, which have limited computing resources, while minimizing the complexity of use for the user. In addition, some of the information necessary to use the SAS, in particular the PIE, is not permanently stored on the UPTD 106 and not included in any data transmissions, so that if the UPTD 106 is lost or stolen, the UPTD 106 cannot be used. Additional details of the SAS and the encryption mechanism are provided with reference to FIG. 4, as follows.

[0064] The internal structure and the generation process of view messages 402, 404 (i.e., UPTF SAS cashless monetary transaction messages) are shown in FIG. 4. The UPTF SAS based views 402, 404 are implemented in software and/or computing hardware as the electronic wireless wallet software application 108 that is executed in the UPTD 106, such as the mobile phone 106. Since the views 402, 404 from the payer and the payee are symmetrical, the payer's 200 view 402 is only described. The symbols used in FIG. 4 are explained below:

[0065] o DIDc: device ID, a unique identifier for the Payer's UPTD device 106 (the consumer (c) or source transaction party).

[0066] o DIDm: device ID, a unique identifier for the Payee's device (the merchant (m) or destination transaction party).

[0067] o RSN: random sequence number.

[0068] o TS: local current timestamp.

[0069] o TID: transaction ID, a unique identification number assigned to an agreement, which is maintained by the STS 120 to identify corresponding UPTF agreement views 402, 404.

[0070] o MD: message digest

[0071] o PIE: Personal identification entry, a user and STS 120 maintained input secret

entry, such as an alphanumeric string. In a typical embodiment described herein, the PIE is only maintained by the user and the STS 120, is not known to and/or maintained by another party to a transaction and/or the financial institutions 122, 204, and is temporally known as an intermediate parameter to the mobile phone 106 of the payer 200 for encrypting the payer view 402. More particularly, the PIE is not included in transaction messages (e.g., UPTF SAS messages and/or SAS based informational messages) and, thus, the wireless wallet software 108 does not transmit the PIE. The PIE can be non-secure by being a substantially short alphanumeric string, such as a 4 digit number. The user enters the PIE whenever the user attempts a transaction. Preferably the PIE is issued to the user following the registration of the user for the application 108 that the client device 106 is used for. The user can also select the PIE at such time. The PIE is an alphanumeric string. In order to speed up the user entry to make it easier for the user to remember it, the PIE can be a number such as 4-digit or 5-digit PIN. The PIE is, however, a piece of highly secure information in the sense that it is never transmitted during the UPTF protocol execution, it is only known to the user and the STS 120, and its secrecy should be well protected. It is assumed that the PIE can be input by the user on a mobile phone 106 in a secure fashion or it may be deterministically generated using a biometric device such as a fingerprint sensor. For example, a computation applied on the fingerprint data received from a fingerprint sensor can be used to generate a PIE that is initially communicated by the user to the STS 120. Whenever the user attempts a transaction, the user applies her finger to the fingerprint sensor, thus generating the PIE. The PIE is not kept in permanent storage on the mobile phone 106, but is used as an intermediate parameter required for the generation of the encryption key for a transaction and it should not be retained by the device 106 for a period longer than the transaction execution time. If a particular implementation of the present invention uses a form of PIE that is not convenient for a user to input for each agreement transaction and the device needs to store its user's PIN, the storage must be secure and tamper-resistant.

[0072] As shown in the FIG. 4, a view 402 comprises a cipher text part (or encrypted part) 406 and a perceptible (e.g., plaintext) part 408. A plaintext part 408 includes the TID, the DIDc of the payer 200 generating the view 402, and the local current timestamp (TS) of device 106. The TS, among other functions described herein, is also used to prevent transaction replay. The encrypted part 406 includes two critical fields: the agreement data and the DIDm of the payee's 202 device 106 involved in the agreement. The DIDm is the minimum necessary reference field in order to provide the desired verification properties of the UPTF protocol. Therefore, a user can execute a UPTD 106 cashless monetary transaction with a transaction party according to a PIE and a wireless wallet software 108

authentication parameter RSN and transaction messages comprising an identifier of the mobile phone, an identifier of the transaction party and an identifier for a transaction (for example, an identifier and/or other transaction related data such as payment amount, etc.) thereby providing the UPTD wireless wallet based upon a combination of the mobile payment software at the UPTD and STS association of the PIE and the software authentication parameter with financial entities of the user and exchange of the transaction messages between the user, the transaction party and the STS 120.

[0073] First, DIDc and the TS obtained from the UPTD's local clock (and/or as provided as a part of the agreement data), are utilized by the device's 106 pseudorandom number generator to generate a time-dependent RSN. Therefore, the parameters of the generator are particular to each device 106. The encryption key K is then generated from the RSN and user input PIE (shown in FIG. 4 with green coloring), where the PIE is generated by the STS 120 as shown in FIG. 1A. Firstly, the RSN and PIE are combined using a function F and then a hash function H is applied to the result (typically a string) to generate the encryption key:

[0074] $K = H(F((PIE, RSN))$

[0075] A message digest function can be applied to the agreement data, the DIDm, and the DIDc to generate a MD of the view. The MD can further strengthen the security by ensuring that no other party has tampered with or modified the contents of the view 402 in any way. The encryption algorithm with the encryption key K is then applied to the MD, the agreement data, the DIDc, and the DIDm to generate the cipher text part of the view 402, as shown in FIG. 4 with yellow coloring. For further protection, the SAS protocol uses random message padding in order to further prevent "known-text" attacks. According to an aspect of the embodiment described herein, the embodiment uses Advanced Encryption Standard (AES) for encryption, a Keyed-Hashing for Message Authentication (HMAC)-based scheme for random number generation, and SHA1 Secure Hash Algorithm for the hash function.

[0076] The STS 120 has sufficient prior knowledge of the functions and specific parameters used by each device 106 in the encryption process, so that when combined with the plaintext portions of a message 402, 404, it is possible to decrypt the message 402, 404 by reversing the above process. For example, from the plaintext part 408 of the view 402, the STS 120 recovers the DIDc and TS, which are used to look-up the customer's 200 PIE and other parameters of the RSN generator that can be stored in the STS database 203. These are used to compute the RSN. The encryption key K can then be computed using the same method with which the customer UPTD 106 generates the encryption key. The cipher text part 406 of the view message 402 is then decoded.

[0077] After all applicable fields of the payer 200 view 402 are acquired, the STS 120 locates the payee's 202 view 404 for the same transaction, using the DIDm and TID included in the previously decoded payer 200 view 402. After going through a similar decryption process, the decoded fields of the agreement data of the payee 202 view 404 are compared with the corresponding fields from the payer 200 view 402. If all applicable corresponding fields match (correspond according to application design), the received views 402, 404 are considered verified. Further processing is then carried out and external executions are triggered as necessary.

[0078] Any responses from the STS 120 to the payer 200 or payee 202 are encrypted by the STS 120 using the same encryption methods and using the parameters for the destination devices 106, 302 and the TS of the original transaction. Only the intended recipient can decrypt the response message, insuring privacy protection and authentication of the STS.

[0079] Another example encryption key generation for the UPTF SAS is described herein. In FIG. 4, using the view 402, the key KEYc is a hash of a RSNc and a PIEc; the detailed key generation procedure is as follows:

[0080] The initialization data for the RSNc are created when a new UPTD account is created by the STS (e.g., when the code executable 108 is created by the STS 120 at operation 110 in FIG. 1A). Specifically:

[0081] 1. a random 128-bit seed is generated using a software service function.

[0082] 2. a random 160-bit initialization timestamp is created also at new UPTD account creation time, using software service function. Therefore, in FIG. 1A, at operation 110, the STS 120 generates device 106 specific initialization parameters of a random number and an initialization time stamp, both of which, at operation 114 are transmitted via the wireless wallet application 108 to the UPTD device 106 (e.g., mobile phone 106).

[0083] In FIG. 1A, at operation 110, the PIE is created by the STS 120 when a new account is created at the STS 120, as follows: a 32-byte random value is created using a software service function , convert each byte to a decimal value string, and concatenate them all to produce a long string. Randomly chop 4 digits from this string to create PIE.

[0084] When the key needs to be created in order to encrypt a transaction message, the following steps take place:

[0085] 1. A 160-bit current timestamp is generated, as follows:

[0086] a. Convert current time to string, for example, converting the current time to a 16

characters string, e.g., 5:04pm, Jan 26, 2004 is written in "0000170401262004."

[0087] b. Take the string and a one way function to output another value, for example by hashing the current time string using SHA1 algorithm, which produces a 160-bit output.

[0088] 2. XOR an init timestamp and current timestamp to produce a 160-bit output. This operation is essentially a form of deterministically calculating a difference between two values of time (i.e., a deterministic transformation between two values).

[0089] 3. Use the 128-bit seed software authentication parameter as data, and the XORed value of the two time stamps as the key, compute the HMAC result (a 160-bit value). The result of the HMAC is the RSNc. Use of the HMAC accommodates unpredictability in the RSNc generation.

[0090] 4. Chop the first 128-bit of the HMAC result, combine (e.g., concatenate) with the 32-bit PIE (convert from a 4 digit string) for a 160-bit value.

[0091] 5. Compute the hash (SHA1) value of the 160 bit stream in operation (4), and chop the first 128 bit as the final key.

[0092] In the encrypted part of the message a hash of the transaction part of the message (with the padding) using SHA1 (alternatively a CRC can be used) is used.

[0093] In the above-described embodiment, the values of a number of bits are provided as unlimiting examples, and the present invention is not limited to a specific number of bits values. Therefore, as illustrated with reference to FIGS. 1, 2, 3 and 4, a UPTF SAS based transaction requires a device 106 which provides device-specific parameters that determine a device-specific and time-specific key and an operator for the device who provides a fixed PIE that is only known to the STS 120 and the operator. The combination of the two is required for an encrypted transaction request that can be validated by the STS 120. Intercepting one (or more) transaction message and successfully decrypting it would not be sufficient for purposes of inferring either the PIE, or the device specific parameters employed in the key generation process. Moreover, a single, time-dependant key is not re-usable because of the pair-wise agreement notion of transactions processed by the STS 120.

[0094] Accordingly, a system and method of generating, by the mobile phone, a first view of the mobile phone cashless monetary transaction, and transmitting the first view of the transaction to the STS according to the SAS; generating, independently by a party to the transaction, a second view of the transaction, and transmitting the second view of the transaction to the STS according to the SAS; and verifying, by the STS, the first and second views to authenticate the transaction, and causing, by the STS, execution of the transaction

based upon the verifying. The first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of time and authentic mobile payment software dependent transformations based upon the PIE, on a transaction message comprising data of the transaction, the identification of the first mobile phone and an identification of a second mobile phone for the second view.

[0095] An authentic mobile phone wireless wallet software 108, which generates the UPTF SAS views, comprises therein software authentication parameters of an initialization time stamp and an initialization random seed number, and wherein the first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction, an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of transformations based upon the PIE and the software authentication parameters included in the authentic payment software from the STS, on a transaction message comprising data of the transaction, the identification of the first mobile phone and an identification of a second mobile phone for the second view. The combination of transformations to encrypt comprises generating a transaction random sequence number based upon the software authentication parameters of the authentic payment software; and generating an encryption key based upon the transaction random sequence number and the PIE.

[0096] The generating of the encryption key further comprises generating a current time stamp; converting the current time stamp to a string; using a one way function, such as a hash function, to convert the current time stamp string to a current time stamp value; determining a time difference value between the current time stamp and the initialization time stamp; computing a Keyed-Hashing for Message Authentication (HMAC) result, based upon the initialization random seed number and the time difference value, to generate the transaction random sequence number; selecting a number of bits from the HMAC result as the transaction random sequence number and combining the selected number of bits fwith the PIE; computing a hash value of the combination; and selecting a number of bits of the hash value to generate the encryption key. The number of bits is about 128.

[0097] FIG. 5 is a flow chart of a UPTF based mobile phone cashless monetary transaction with a merchant, according to an embodiment of the present invention. A computer system is described that comprises an Online Payment Service (122, 204), a Secure Transaction Server (STS) 120, and a mobile phone wireless wallet application 108

comprising mobile phone specific electronic financial transaction initialization parameters, that is downloadable to a mobile phone 106 for consumers to execute a mobile phone cashless monetary transaction with a merchant, send money to other consumers using their mobile phone or for consumers to request money from other consumers using their mobile phone. When making payments using a mobile phone, the consumer can select any of the accounts registered with the online payment service 122, 204 to make the payment using that account.

[0098] An Online Payment Service (OPS) 122, 204 is a web accessible service that enables consumers to make payments to other consumers or merchants, or consumers or merchants to request payments from other consumers. In current Online Payment Services 122, 204, a consumer 200 identifies a merchant 202 or another consumer 200 by an e-mail address (or some other user identifier, such as a user name, etc.) that has been verified by the OPS 122, 204. Users 200, 202 of the OPS 122, 204 provide to the online payment service 122, 204 the information of their personal accounts (credit cards, bank accounts, etc.), so that any of those accounts can be used when making a wireless device cashless payment. The Secure Transactions Server (STS) 120 is a Universal Pervasive Transaction Framework (UPTF) based system that verifies transaction requests that observe the UPTF.

[0099] As also described above with reference to FIG. 1B, when the user is logged on, over the web, to the OPS 122, 204, the user might see an option that enables them to make payments or request payments from a mobile phone 106. Upon following the link associated with this option, the user will be asked for the phone number of the mobile phone 106 that she would like to use for such transactions and possibly the mobile carrier for that phone number. Upon submitting this information, the user will be shown a PIE to be used for making payments and requesting money from her mobile phone 106 and she will also receive a SMS (Short Messaging Service) message on the specified mobile phone, with a link that if followed will enable her to download to her mobile phone 106 the mobile phone wireless wallet software 108 that will enable her to make payments and request money using her mobile phone 106. The link points to a unique downloadable executable associated with this user at the STS 120 via the STS 120 maintained software authentication parameters and PIE. If the user has access to the web from the mobile phone 106, she will be able to follow that link and download the software 108 to the mobile phone 106. Upon completing the download of the mobile phone wireless wallet application 108, the user will be asked to save the application on the mobile phone 106. From that point on the application 108 is ready for use. The downloaded application can be referred to as mobile phone electronic wireless wallet 108. A consumer 200 who is also an OPS 122, 204 user and has

downloaded a mobile phone wireless wallet 108 to her mobile phone 106 will be referred to as a mobile OPS user (as opposed to a OPS user). All mobile OPS users are also OPS users, so when using the term OPS users, it refers to both OPS users and mobile OPS users.

[00100] As discussed above with reference to FIG. 1A, the mobile phone wireless wallet software 108 is an executable written in a language that is installable and executable on the mobile phone 106, such as Java 2 Platform, Micro Edition (J2ME), Binary Runtime Environment for Wireless (BREW), any other language that might be installable on the mobile phone 106 so that applications written in that language can be executed on the mobile phone 106, or any combination thereof. The executable 108 is created by the STS 120 entirely, or at least partially as the STS 120 needs to create, store and retrieve data that is used to identify this executable 108 and the user associated with it for each future transaction. The STS 120 also creates and stores the PIE that is used for such transactions. The PIE is not stored on the executable 108 or the mobile phone 106 that this executable 108 will be eventually downloaded to. Only the software authentication parameters (operations 50, 52) are included in the mobile phone wireless wallet software 108.

[00101] Also, an OPS user can make a payment from the web-accessible OPS 122, 204 to a mobile OPS user, by using the mobile phone number of the mobile OPS user to identify the consumer who will receive the payment. Typically, OPS users identify other OPS users with an e-mail address. If an OPS user knows the mobile phone number of a mobile OPS user, she can identify that user by the mobile phone number and makes a payment to that user. Similarly if an OPS user wants to request money from a mobile OPS user, she will have to identify that user by a mobile phone number. In the latter case, the mobile OPS user might receive a SMS notification on her mobile phone notifying her that someone has requested money from her. The requestee can the use her mobile phone 106 to make a payment to that OPS user.

[00102] Also a mobile OPS user can use her mobile phone the make payments to other OPS users. If the payee is also a mobile OPS user, the payer can identify the payee by mobile phone number, although she can also identify that payee by e-mail address if she so chooses. Entering a phone number in a mobile phone is easier and faster than typing an e-mail address. If the payee was identified by phone number, the payee will receive a SMS notification about the payment. The payer also will receive a notification SMS if the payment is successful. The payer can select any of the OPS-registered accounts to make the payment from.

[00103] A mobile OPS user can also use her mobile phone to request a payment by an

OPS user, by similarly specifying the OPS user by either e-mail address or mobile phone number if the user knows it. Requestor and requestee will receive a SMS message notifying them of successful request. Mobile OPS users can also view in their mobile phone a list of transactions that involved their mobile wireless wallet software 108 from a relevant menu of the application 108. This list can include all transactions that involved the mobile phone 106 in order to effect the transaction. Specifically, this includes payments that were made from the mobile phone 106 (including a payment made in response to a request for payment) and requests for payments to other OPS users. OPS users can view in the web-accessible OPS, a list of all transactions that they have performed, regardless of whether they were made from the web-accessible OPS or from their mobile phone 106.

[00104] Payments and request for payments from the mobile phone 106 using the mobile phone wireless wallet software 108 result in UPTF messages (e.g., 402, 404), encrypted according to UPTF, send by the mobile phone's 106 wireless wallet 108 to the STS 120 and/or generated by the STS 120 (i.e., in case of a person-to-person mobile phone payment, the STS may or may not create a second view for the payment transaction depending on system configuration and/or application design and/or transacting party preference). For example, in FIG. 5, in case of a member-to-member, as a person-to-person transaction example, cashless payment transaction involving one payment service 122, 204 in which both members have registered accounts, the merchant 202 transaction system 302 and the payment service 122, 204 could be logically (conceptually) one entity/system 500 for through processing (via a channel D between the OPS 122, 204 and the STS 120) the UPTF views 402, 404 to/from the STS 120. In general, in a person-to-person type transaction scenario, each transacting party creates its own view. In case of a payment by one person to another person using the mobile phone wireless wallet 106, because the other person (payee) may not require (or be required) to approve a payment made to the payee, the payee might not need to create a view to accept the payment. Therefore, in case of a payment transaction, the payee's view can be omitted and the STS 120 may simply only verify a first payment request view 402 from a payer 200, or the STS 120 may create the other person's (payee 202) second view 404 on the payee's behalf. Paired views 402, 404 are used in case of a plurality of online payment services 122, 204 to achieve person-to-person mobile payment transactions. According to an aspect of the embodiment described, the system 500 can also comprise the STS 120. Also, responses to messages from the STS 120 to a mobile phone 106 are UPTF SAS messages, encrypted according to UPTF SAS. The OPS 122, 204 has a secure connection (i.e., channel D) to the STS 120.

[00105] According to an aspect of the embodiment described herein, in case of person-to-person payment transaction, a payment action from the web-accessible OPS 122 (i.e., in case of a payment from a desktop to a mobile phone wireless wallet 106), 204 can be carried through the secure connection D to the STS 120 and need not be encrypted according to UPTF SAS. As discussed above, payment from the web-accessible OPS is effective immediately and does not require an action by the payee. Still, the STS 120 will receive that payment action, decrypt the payment action, which according to the UPTF SAS serves to authenticate the originating payment action requester, including the transaction, and will determine if the payee is a valid mobile OPS user, who is still active with the STS 120, and possibly notify the payee 202 mobile phone wireless wallet 106.

[00106] According to another aspect of the embodiment described herein, the STS 120 through the secure connection D between the STS 120 and the OPS 122, 204, can receive a request for payment to a mobile OPS user (i.e., in case of a request for payment from a desktop to a mobile phone wireless wallet 106). Upon receipt of the request the STS 120 will send a notification SMS to the mobile phone 106 of the mobile OPS requestee. When the mobile OPS user, using her mobile phone 106 and the mobile phone wireless wallet software 108 checks for pending requests she will see that request and can decide to make a payment to the requestor. Upon receipt of the payment message by the STS 120, the STS 120 will check against the pending request by the request, will determine according the UPTF methods that the complete transaction is valid and accordingly notify requestor and requestee.

[00107] According to another aspect of the embodiment described herein, a request for payment by a mobile OPS user that uses her mobile phone for that request, is handled similarly. If the requestee was identified as a mobile OPS user, the requestee will receive a notification SMS and will see the request upon checking for pending requests with the wireless wallet software 108 and can decide to complete a payment. The STS 120 will use the UPTF criteria to compare with the requestor's messages to the STS 120 and determine the validity of the complete transaction. Upon such determination the STS 120 will notify the OPS and the requestor and requestee.

[00108] All of the above described transaction examples, only require that the mobile OPS user use her mobile phone 106 and the mobile phone wireless wallet software 108 and entering the designated PIE for those transactions. The STS 120 and OPS 122, 204 may be operated by the same entity and/or execute in the same computer system, or they me be operated by different entities. According to an aspect of the embodiment(s) described herein, a user can be notified at the mobile phone wireless wallet 106 of a status (e.g.,

result, confirmation, state, success/failure, problem/help notification, etc.) of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message.

[00109] FIG. 6 is a flow chart of a UPTF based mobile phone cashless monetary transaction to purchase a movie ticket, according to an embodiment of the present invention. FIGS. 7A-B are mobile phone display screen user interface images to execute mobile phone cashless monetary transaction to purchase a movie ticket and to obtain, store and retrieve a transaction receipt, according to an embodiment of the present invention. With reference to FIGS. 5, 6, and 7A-7B, an example mobile phone cashless monetary transaction with a merchant is described. In FIG. 5, at operation 502, a mobile phone 106 user/consumer 200 uses an installed (FIGS. 1A, 1B, 1C) mobile phone wireless wallet 108 to request a purchase order from the merchant 302 payee 202. In FIGS. 5 and 6, operation 502 comprises binding the consumer 200 with the merchant 302 transaction information, for example, by browsing a merchant ticket sales application (merchant transaction server (MTS)) 302 (FIGS. 2, 3) for purchasing a movie ticket via a mobile phone (cellular) communication network. The binding of the user with a merchant's virtual shopping cart can also be performed by inputting at the mobile phone wireless wallet software 108 an identifier for the merchant (e.g., a POS 135 transaction paper receipt information) and/or the mobile phone wireless wallet might have pre-stored a merchant identifier (e.g., Internet Universal Resource Locator (URL) address). In FIG. 7A, for example, at operation 502, mobile phone user interface screen images 702a-h are displayed for browsing the merchant ticket sales application 302, which comprise, at 702a, selecting the mobile phone wireless wallet software 108, at 702b, selecting "Go shopping," at 702c, selecting "Movie Theater," at 702d, selecting "Movies Playing Next," at 702e, selecting movie times from displayed movie time information, at 702f, selecting a movie from displayed movies at the selected time, and, at 702g, completing a purchase order form request to be sent to the merchant 302, and, at 702h, transmitting to the merchant 302 the purchase order request , which is a binding of the consumer 200 with the merchant 302 transaction information by identifying what is being paid for (electronic shopping cart) and payment information.

[00110] At operation 504, the mobile phone wireless wallet software 108 receives a purchase order from the merchant ticket sales application 302, which, for example, can result in mobile phone user interface screen image 704 that displays a summary of the electronic shopping cart, including payment information, from the merchant 302, and a "Please press PAY button" selection. According, to an aspect of the invention, at operation 504, information used as a device identifier of the merchant (DIDm) (FIG. 4) can be identified

by the mobile phone wireless wallet 108 based upon the purchase order received from the merchant 302 payee 202.

[00111] At operation 506, selection of the "PAY" button at 704 begins the UPTF SAS functions of the embodiment. In particular, via the mobile phone user interface screen images 706a, 706b, the mobile phone wireless wallet software 108 requests input of the PIE (e.g., a PIN) and generates a UPTF SAS view 402 (as described with reference to FIG. 4), as a consumer 200 REQuest transaction, and transmits the REQuest transaction to the merchant 302. As shown in FIG. 6, the UPTF SAS based messages 402 from the mobile phone wireless wallet software 108 are carried over the mobile carrier's network, either directly to the STS 120 or indirectly through the merchant application 302, as indicated by Channel B. The transport layer between client 108 and MTS 302 and/or STS 120 uses Internet (Internet Protocol) HTTP communication. However, the transport layer can by any known transport layer, such as HTTP, web service calls, socket based communication, etc. According to an aspect of the embodiment(s) described herein, the MTS 302 is implemented with a web interface for sending and receiving messages from and to the mobile phone client 106; specifically the mobile phone wireless wallet software client 108 running on the mobile phone 106 sends its messages to the MTS 302 by submitting them to a pre-specified CGI-like interface, and the MTS 302 forwards/receives the same/responses to/from the STS 120 using web service calls. In other words, a UPTF message is an HTTP parameter. Since HTTP is stateless, the MTS 302 uses a small database to keep track of state(s) during the sending and receiving the messages. Also, because messages are carried over HTTP, a hex encoding of the encrypted UPTF SAS based message is used to avoid problems with special ASCII characters in the encrypted form of the message, as it is transported over HTTP.

[00112] At operation 508, the MTS 302 generates an MTS UPTF SAS view 404, as an MTS REQ, and transmits the MTS REQ and the Consumer REQ (i.e., views 402, 404) to the STS 120. According to an aspect of the embodiment, at operation 506, information used as a device identifier of the consumer (DIDc) is obtained by the MTS 302 from the unencrypted part of the consumer REQuest view 402, based upon which the MTS 302 generates the MTS REQuest view 404.

[00113] At operation 510, the STS 120 gets abstracted account listing for the consumer 200 from the payment service 122, 204. In particular, if at 706b, the consumer 200 inputs a request to use a financial account other than a default account, the consumer REQuest view 402 includes a request for financial account information. At operation 510, the STS 120 uses an account association 123 for the consumer 200, which is provided from the payment

service 122, 204 (i.e., operations 105 in FIG. 1A), to confirm the consumer REQuest with the payment service 122, 204. At operation 512, the STS 120, receives an account reference listing (not actual account numbers) from the payment service 122, 204. At operations 514, 516, the STS 120 forwards via the MTS 302, an STS Response to the consumer REQuest view 402, which includes the account reference listing. At operation, 516, the mobile phone user interface screen image 708 displays a selectable user account reference listing. At operation 518, the consumer 200 authorizes the transaction. At operation 520, the MTS 302 sends an MTS authorization and the consumer authorization to the STS 120.

[00114] At operation 522, in response to the MTS and consumer authorization requests of operation 520, the STS 120 sends an AUTHorization transaction to payment service 122, 204 and, at operation 524, receives a payment service response. At operation 526, the STS 120, forwards to the MTS 302 the payment service response to the AUTHorization transaction, which, at operation 528, the MTS 302 forwards the STS response to AUTHorization transaction to the consumer 200. In particular, at operation 528, the mobile phone user interface screen image 710 displays a transaction success confirmation message. Accordingly, at operations 508 and 520, the STS 120 receives and verifies the UPTF SAS based merchant and consumer views 402, 404 (e.g., decrypting and cross-referencing the UPTF SAS based MTS REQ and consumer REQ messages and the MTS AUTH and consumer AUTH messages).

[00115] According to an aspect of the described embodiment herein, the wireless wallet application 108 running on the mobile phone 106 receives receipt related information, as shown in the display screen image 712, which according to an aspect of the embodiment is in the form of a barcode image on a computer display screen, as shown in a barcode image 714 displayed on the mobile phone display screen 106, after every successful purchase and stores these receipts on the mobile phone 106 for further reference and reuse (e.g., to be displayed on a display screen of the mobile phone wireless wallet 106 and read from the computer displayed barcode image by a barcode reader 315 to gain physical access to the paid service at a physical merchant service spot, such as a cinema point of sale (POS) 315). The transaction receipt related information could be remotely stored and retrievable. Therefore, the wireless wallet application 108 provides transaction receipt management and in FIG. 7B, an example of mobile phone display screen user interface images 716a-d is illustrated for retrieving transaction receipt related information. According to another aspect of the embodiment(s) described herein, provided is a system and method of notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice

message, including transaction receipt information, wherein the receipts can be forwarded to another (e.g., in case of a movie ticket purchase, a barcode image movie ticket receipt delivered to the mobile phone wireless wallet 106 can be forwarded to another person for theater entry). Therefore, the wireless wallet software 108 includes a general receipt management mechanism based upon a computer display screen image of a barcode 714. In FIG. 6, the VPN is a Virtual Private Network.

[00116] The wireless wallet application 108 running on the mobile phone 106 combines both a browser and a payment application. The browser (lightweight web client) is used for purchasing and the payment application component is used for executing a UPTF SAS transaction.

[00117] FIG. 8 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment transaction, according to an embodiment of the present invention. FIG. 9 is a flow chart based upon mobile phone display screen user interface images and message flow between a requestor device, a secure transaction server (STS) and a requestee to execute a person-to-person mobile phone cashless payment request transaction, according to an embodiment of the present invention. FIG. 10 is overall mobile phone display screen user interface images and possible workflows available to an operator of a wireless wallet on a mobile phone to execute person-to-person cashless monetary transactions, according to an embodiment of the present invention. FIGS. 11-12 are diagrams of mobile phone person-to-person cashless monetary transaction message formats to execute various mobile phone cashless monetary transactions, according to an embodiment of the present invention. An example of a person-to-person payment and a person-to-person payment request will be described with reference to FIGS. 8, 9, 10 and 11. FIG. 8 is a flow chart of a person-to-person payment when a mobile phone payer 200 makes payment via a payment request or via responding to a received request for payment from a payee 202. In FIG. 8, at operation 802, a mobile OPS payer 200 starts the mobile phone wireless wallet 108 and chooses option "P2P Payment," corresponding to the mobile phone user interface display screen image 1002 (Form 0). At operation 804, the user selects option "Make Payment," corresponding to the mobile phone user interface display screen image 1004 (Form 1). Also, at operation 806, the user can select option "Pending Requests," corresponding to the mobile phone user interface display screen image 1004 (Form 1). If, at operation 804, the user selects "Make Payment," at operation 810, the user is prompted, via the mobile phone user interface display screen image 1006 (Form 2), to enter a phone number/email address. After

operation 804 and operation 806 (as the case may be), the user is prompted, via the mobile phone user interface display screen images 1010 (Form 4) or 1018 (Form 7), to enter a PIE, such as a PIN. At operation 812, when the user enters the PIN, the mobile phone wireless wallet software 108 uses the input PIN to create encrypted payee id request/pending list request (as the case may be) according to UPTF SAS message view 402 and sends the message view 402 to the STS 120. At operation 814, the STS 120 receives the message views 402 and authenticates the user payer 200, and identifies payee 202/returns a pending request list (as the case may be).

[00118] At operation 814, the STS 120 creates and transmits response requests to a "payment request" or a "pending payment request list," according to UPTF SAS message views 402. At operation 816, in case of a "payment" transaction, the mobile phone wireless wallet software 108 receives from the STS 120 a payee id (e.g., udid, id, fullname), and the user is prompted, via the mobile phone user interface display screen images 1012, 1014 (Forms 5, 6), respectively, to enter amount the user payer 200 wants to pay and confirm. At operation 818, in case of a "pending payment requests" transaction, the mobile phone wireless wallet software 108 receives from the STS 120 a pending payment request list, and the user is prompted, via the mobile phone user interface display screen images 1016, 1018 (Forms 8, 6), respectively, to select from a pending payee payment request list and confirm. At operation 814, for a make payment transaction, if a payee 202 confirmation message view 404 is not required, the STS 120 only authenticates payer 200 message view 402 and identifies payee 202. At operation 814, for a make payment transaction in response to a payment request from another person, the STS 120 verifies both message views 402, 404 of the payer 200 and the payee 202, respectively, according to the UPTF SAS.

[00119] At operations 816 and 818, the mobile phone wireless wallet software 108 sends a payment message view 402 that comprises payer, payee and amount information, and, at operation 820, the STS 120 receives and processes the payment message view 402 (display screen image 1020), and returns a final result to payer 200. If the payment transaction is successful, the payee 202 can be notified as well. In particular, at operation 822, the mobile phone wireless wallet software 108 receives a payment result message view 402 and informs the user payer 200, via the mobile phone user interface display screen image 1022b (Form 10), of the payment result and ask if the user wants to bookmark payee. At operation 820, a notification to payee 202, via SMS or email, can be sent.

[00120] FIG. 9 is a flow chart of a person-to-person payment when a mobile phone payee 202 requests payment from a payer 200. In FIG. 9, at operation 902, a mobile OPS payee 202 starts the mobile phone wireless wallet 108 and chooses option "P2P Payment,"

corresponding to the mobile phone user interface display screen image 1002 (Form 0). At operation 904, the user selects option "Request Payment," corresponding to the mobile phone user interface display screen image 1004 (Form 1). At operation 906, the user is prompted, via the mobile phone user interface display screen image 1006 (Form 2), to enter a phone number/email address for the payer 200. Also, at operation 908, the user can be prompted, via the mobile phone user interface display screen images 1006 and 1008 (Forms 2 and 3), respectively, to select a payer 200 from a favorite list. After operation 906 and operation 908 (as the case may be), the user is prompted, via the mobile phone user interface display screen image 1010 (Form 4), to enter a PIE, such as a PIN. At operation 910, when the user enters the PIN, the mobile phone wireless wallet software 108 uses the input PIN to create encrypted payer identification request according to UPTF SAS message view 402 and sends the message view 402 to the STS 120. At operation 912, the STS 120 receives the payer identification request message view 402 and authenticates the user payee 202, identifies payer 200 and resolves payer 200 information and returns payer 200 information to the mobile phone wireless wallet software 108.

[00121] At operation 912, the STS 120 creates and transmits response requests according to UPTF SAS message view 402. In particular, at operation 912, the STS 120 creates a payer 200 information (e.g., udid, id, full name) response message view 402. At operation 914, the mobile phone wireless wallet software 108 receives from the STS 120 the payer 200 information (e.g., udid, id, fullname), and the user is prompted, via the mobile phone user interface display screen images 1012, 1014 (Forms 5, 6), respectively, to enter amount the user payee 202 asks to be paid from the payer 200 and confirm.

[00122] At operations 914, the mobile phone wireless wallet software 108 sends a payment request from payer 200 message view 402 that comprises payer, payee and amount information, and, at operation 916, the STS 120 receives and processes the payment request from payer 200 message view 402 (display screen image 1020). At operation 916, the STS 120 processes (i.e., decrypting according to SAS and logging) the received payment request from the mobile phone wireless wallet software 108 by creating a new payment request entry for the payer 200, which can be requested by the payer via operation 806. In particular, at operation 916, the STS logs a transaction identifier of the message view 402, and with reference to FIG. 8, at operation 806, the payer 200 can select "Pending Payment Requests" to receive the created payment request, including the transaction identifier, of operation 916. In FIG. 8, via operations 812, 814 and 816, the payer 200 creates a corresponding agreement view 404, including the transaction identifier of the payment request, which corresponds to the created payment request of operation 916 and

can be processed by the STS 120 according to UPTF SAS by decrypting and verifying both views 402, 404 of the payer 200 and payee 202, respectively. At operation 916, if payer 200 is a mobile phone wireless wallet software 108 user, SMS can be sent to the payer 200 or otherwise an email notification can be sent to the payer 200. At operation 916, the STS 120 returns a request result to payee 202. In particular, at operation 918, the mobile phone wireless wallet software 108 receives a payment request result message view 402 and informs the user payee 202, via the mobile phone user interface display screen image 1022a (Form 10), of the payment request result and ask if the user wants to bookmark payer.

[00123] More particularly, FIG. 11 is a format diagram of six example mobile phone person-to-person cashless monetary transaction message views 402, 404, including unencrypted part 408 and encrypted part 406, for executing mobile phone person-to-person payment transactions. In FIG. 11, according to an aspect of the embodiments described herein, messages A and C are informational message views that are essentially SAS messages (encrypted according to SAS, which authenticates a sender of a message and the content). Responses from the STS 120 to the mobile phone wireless wallet 106 (messages B, D, and G) are also SAS messages (encrypted according to SAS, which authenticates a sender of a message and the content) (i.e., the messages are encrypted with a generated key (FIG. 4) corresponding to the device 106, even though the messages are sent by the STS 120, thus from the device 106 perspective, authenticating the sender (the STS 120 in this case) and the content, because only the corresponding device 106 with the installed authentic wireless wallet software 108 (via software authentication parameter(s) and the STS 120 can possibly successfully reconstruct the key used for encrypting a message at a particular time (timestamp). Messages E/F are essentially agreement message views (a transaction message, including a transaction identifier, for an agreement that involves or relates to two or more parties) that comply with UPTF and are also secured according to SAS encryption, hence UPTF SAS. Therefore, in the embodiments described herein, mobile phone transactions are executed according to SAS as well as UPTF SAS. For example, message A is a pending payment request list message view 402 created at operation 806, which is provided after operation 812 to the STS 120. Message B is a pending payment request list reply message view 402 created at operation 814 by the STS 120. Message C is a person (e.g., peer) identification request message view 402 created at operation 810 by the mobile phone wireless wallet 108, which is provided after operation 812 to the STS 120. Message D is a person (e.g., peer) identification reply message view 402 created by the STS 120 at operation 814, which is transmitted to the mobile phone wireless wallet software 108 at operation 816. Messages E/F are make payment request/request payment request message views 402 created by the mobile phone wireless wallet software 108 at operations

816 and 818, respectively, and transmitted to the STS 120 for processing at operation 820. Message G is a transaction result message view 402 created by the STS 120 at operation 820, which is transmitted to the mobile phone wireless wallet software at operation 822.

[00124] FIG. 10 illustrates and describes three possible flows for mobile phone user interface display screen images. In FIG. 10, flow I is mobile phone user interface display screen images 1002, 1004, 1006, 1008, 1010, 1012, and 1014. In FIG. 10, flow II is mobile phone user interface display screen images 1002, 1004, 1006, 1010, 1012 and 1014. In FIG. 10, flow III is mobile phone user interface display screen images 1002, 1004, 1018, 1016 and 1014. FIG. 12 is a diagram of an example envelope of a mobile phone cashless monetary transaction message view 402 for a pending payment request list reply (Message B in FIG. 11). In FIG. 12, the message B view 402 is according to the SAS. The "message" portion contains an actual content of a message, as encrypted according to SAS. FIG. 12 shows example of message B (FIG. 11) for a Pending Payment Request List Reply. The message format 1202 is an example format of the "message" portion for a Pending Payment Request List Reply message B sent by the STS 120 in reply to message A. The message format 1202 comprises a list of pending payment requests and a list of abstracted account identifiers to select from for payment. Padding 1 and padding 2 can be random numbers to hide location of the "message" portion. Ptr1 and ptr2 are pointers indicating where the "message" portion begins.

[00125] A true mobile (service spot independent) electronically anonymously authenticable wireless wallet 106 is provided in which the user does not carry any financial account information, the mobile device does not temporally and/or permanently store any actual user financial account information, the mobile device does not require/need to be swiped over and/or even interface with a point of sale (POS) reader (i.e., a user is not bound to a payee location) to execute mobile authenticable cashless monetary transactions, and no bank card swiping is performed by the user at the mobile device and/or via the mobile device. A mobile phone, comprises a computer readable medium storing a mobile payment software initialized at a secured transaction server (STS) with a software authentication parameter, as an authentic mobile payment software; and a programmed computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising prompting a user to input a personal identification entry (PIE) that is correlated by the STS with a phone number of the mobile phone and the authentic mobile payment software, and generating according to the PIE and the software authentication parameter a transformed authenticable mobile phone cashless monetary transaction, as a mobile phone wireless wallet of the user of the mobile phone, thereby

accommodating mobile phone UPTF SAS based transactions.

[00126] Although the above-described embodiments are directed to mobile phone user electronically authenticable cashless monetary transaction, the embodiments are not limited to cashless monetary transactions, any type of user electronically authenticable transaction can be accommodated. The user mobile phone wireless wallet 106 provides an always-on, always-available, always-accessible "footprint" for accessing, delivering and paying (for) services with selectable accounts. The "footprint" is an authentic mobile phone wireless wallet application 108 according to a mobile phone application platform, such as J2ME, and running on a consumer's mobile phone 106. The authentic mobile phone wireless wallet application 108 can be distributed and managed directly by the "business" without the collaboration, participation and consent of a mobile phone communication carrier. The services that include "sensitive" data, such as payment, are securely accessible by the user, with a simple user maintained (i.e., not permanently stored on the mobile phone 106) identifier, such as a 4 digit PIN. Further, a provider-controlled "footprint" for additional services beyond payment can be accommodated.

[00127] For example, in case of a movie ticket purchase service using the user mobile phone wireless wallet 106, a main service would be payment for movie ticket at any location (mobile) and redemption at a service spot in the movie theater to gain entry admission. Some example additional services can be browsing movie schedules prior to purchasing, rating of movies for a reward (discount) to be applied towards future purchases, loyalty programs with immediate awards, download previews, and provide notifications of movie times based on customer profile. Also, ability to send notifications (SMS) for promotions/advertisements that are accessible once starting the mobile phone wireless wallet application 108 and/or redeemed with the wireless wallet application 108 (e.g., in combination with payment towards something that is paid for and the promotion is applied towards).

[00128] Other example mobile phone wireless wallet application 108 services comprise financial related transactions for person-to-person and customer-online merchant. Additional services can be online auction related services, such as initial informational services for an online auction service customer, checking watched auctions, etc., and payment to another transaction party for a successful bid. Also, ringtone, game, digital/media content, software, advertisements, coupons, etc. rewards mechanism (or credits for ringtone, game, digital content/media, software, etc. purchasing) can be provided in connection for mobile to mobile payments using the mobile phone wireless wallet application 108. More particularly, according to an aspect of the embodiment(s) described herein, a system and method is

provided that ties transactions with a wireless wallet 106 (e.g., wireless wallet software 108 payment transactions/purchases) to a reward system for receiving/purchasing mobile phone related items, such as ringtone, game, digital/media content, software, etc. According to another aspect of the embodiment described herein, a mobile phone reward system and method is provided in which a reward is immediately deliverable to a mobile phone, for example, after completion of a wireless wallet 106 payment, an automatic ringtone download, via a mobile phone communication network, to the mobile phone 106. The mobile phone wireless wallet application 108 makes the process of earning and redeeming credits much easier. Customers can be online payment services, banks, credit card companies, online merchants, and/or physical merchants using a mobile phone wireless wallet 106 as a point of sale (POS).

[00129] Other example mobile phone wireless wallet application 108 services comprise ordering and payment for medical prescriptions and refills prior to pickup at an authorized merchant. Additional services of notification (SMS) of refill due, when ready for pickup, rewards, transfer prescriptions by providing doctor's identifier and prescription number from mobile phone and incorporating validation of doctor and prescription.

[00130] Other example mobile phone wireless wallet application 108 services comprise payment, in-store, using the store loyalty card with the mobile phone wireless wallet 106, along with additional services of augmenting a royalty program, delivering and accessing rewards, coupons, etc. and redeeming.

[00131] Other example mobile phone wireless wallet application 108 services comprise various types of financial transactions, such as browsing accounts, funds, stocks, selling, buying, transferring stocks/funds/bonds using funds, broker accounts, banks, debit/credit cards. Additional services of notification onto the mobile phone wireless wallet 106 if stock meets price range, delivering and accessing recommendations, reports, analysis, trends, tracking, and voice activation.

[00132] The above-described processes of the present invention are implemented in software and/or computing hardware. The embodiment(s) described herein can be thought of as a server-side wallet to which access can be controlled through a four digit PIN, with the UPTF notions of multi-party agreements and time-of-transaction dependent key generation combining to provide expected security properties. The combined solution does not require any storage of critical data on the mobile device, it does not impose special hardware requirements and "reduces" security to a 4-digit PIN which is a major convenience for the user. The mobile phone wireless wallet described herein is computationally fast; on mobile phones the key generation and encryption (or decryption) (i.e., SAS portion) can take

approximately 100 ms on a fast available mobile phone (approximately 500 ms on a slow mobile phone) using J2ME for 160-bit AES encryption for each message. Thus, the security-related computational time is non-noticeable with respect to the transaction time (time it takes for messages to travel over a communication link).

[00133] In view of the above described examples of preferred embodiments, a computing device 106 suitable for use in implementing the present invention can be any electronic computing device (a programmable electronic device that can store, retrieve, and process data) allowing mobile (wireless) telecommunication with other computing devices and having one or more communicably connected components of computer/computing processors, such as Central Processing Units (CPUs); input unit(s)/device(s) (e.g., microphone for voice command/control, etc., keyboard/keypad, pointing device (e.g., mouse, pointer, stylus), touch screen, etc.); output unit(s)/device(s) (e.g., computer display screen (including user interface thereof, such as graphical user interface), speaker(s), printer(s), etc.); computer network interface(s), including known communication protocols thereof, (e.g., mobile telephone (voice/data (Internet)) (cellular radio networks, satellite, etc.) network, radio frequency technology, local area network, etc.); and computer readable recording media to store electronic information, such as software (e.g., operating system, wireless wallet software 108) and/or electronic data (any known computer readable media, such as volatile and/or non-volatile memory (Random Access Memory), hard disk, flash memory, magnetic/optical disks, etc.) for execution by computer/computing processors and/or electronic circuitry.

[00134] The many features and advantages of the invention are apparent from the detailed specification and, thus, it is intended by the appended claims to cover all such features and advantages of the invention that fall within the true spirit and scope 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 illustrated and described, and accordingly all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

CLAIMS

What is claimed is:

1. A method, comprising:

initializing, at a secure transaction server (STS), a mobile payment software with a software authentication parameter, as an authentic mobile payment software;

providing an STS correlation between a personal identification entry (PIE) and the authentic mobile payment software;

installing, in a mobile phone, the authentic mobile payment software; and

inputting, by a user, the PIE to the installed authentic mobile payment software to generate according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone.

2. The method of claim 1, further comprising implementing the authentic mobile payment software according to an application platform of the mobile phone.

3. The method of claim 1, further comprising implementing the authentic mobile payment software according to Java 2 Platform Micro Edition (J2ME) and/or Binary Runtime Environment for Wireless (BREW).

4. The method of claim 1, further comprising:

providing to the mobile phone a download link to the authentic mobile payment software; and

downloading to the mobile phone the authentic mobile payment software via the download link, thereby performing the installing of the authentic mobile payment software.

5. The method of claim 4, wherein the authentic mobile payment software downloaded link is transmitted to the mobile phone using short/multimedia message service.

6. The method of claim 1, wherein the mobile phone authenticable cashless monetary transaction is performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol.

7. The method of claim 1,

wherein the authenticable mobile phone cashless monetary transaction is performed

according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol,

wherein the initializing of the authentic mobile payment software comprises:

providing to the user a mobile phone cashless monetary transaction activation link at a computing device;

registering a phone number of the mobile phone of the user via the activation link;

transmitting the registered phone number of the mobile phone to the STS;

generating, by the STS, an executable mobile payment software including the initialization parameter, as the authentic mobile payment software; and

generating, by the STS, the PIE correlated in the STS with the authentic mobile payment software, and

wherein the installing of the authentic mobile payment software download link comprises:

transmitting, by the STS, via short/multimedia message service using the registered mobile phone number, a download link to the authentic mobile payment software to the mobile phone of the user;

downloading to the mobile phone the authentic mobile payment software via the download link, thereby performing the installing of the authentic mobile payment software; and

providing, by the STS, the PIE to the user.

8. The method of claim 6, further comprising:

correlating, at the STS, abstracted registered financial entities information of the user with the authentic mobile payment software;

binding the authentic mobile payment software with transaction information of a transaction party;

presenting, by the STS at the mobile phone, a selectable list of abstracted identifiers corresponding to the registered financial entities of the user correlated with the authentic mobile payment software; and

executing the mobile phone cashless monetary transaction with the transaction party using the PIE and the software authentication parameter and according to UPTF transaction messages that comprise an identifier of the mobile phone, an identifier of the transaction party, and an identifier of the transaction, thereby providing the mobile phone wireless wallet based upon a combination of the authentic mobile payment software at the mobile phone and the STS correlations of the authentic mobile payment software with the PIE, the

software authentication parameter, and the financial entities of the user, and exchange of the UPTF transaction messages between the user, the transaction party and the STS.

9. The method of claim 6, wherein the UPTF SAS comprises

generating, by the mobile phone, a first view of the mobile phone cashless monetary transaction, and transmitting the first view of the transaction to the STS according to the SAS;

generating, independently by a party to the transaction, a second view of the transaction, and transmitting the second view of the transaction to the STS according to the SAS; and

verifying, by the STS, the first and second views to authenticate the transaction, and

causing, by the STS, execution of the transaction based upon the verifying.

10. The method of claim 9, wherein the first and second views are symmetrical and the SAS comprises generating as each independent view of the transaction an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of time and authentic mobile payment software dependent transformations based upon the PIE, on a transaction message that comprises data of the transaction, the identification of the first mobile phone and an identification of a second device for the second view.

11. The method of claim 9,

wherein the software authentication parameter comprises a plurality of parameters of an initialization time stamp and an initialization random seed number, and

wherein the first and second views are symmetrical and the SAS comprises:

generating as each independent view of the transaction, an unencrypted perceptible part comprising an identification of a first mobile phone for the first view and a current timestamp, and an encrypted part by performing a combination of transformations based upon the PIE and the software authentication parameters included in the authentic payment software by the STS in the initializing, on a transaction message that comprises data of the transaction, the identification of the first mobile phone and an identification of a second device for the second view.

12. The method of claim 11, wherein the combination of transformations to encrypt comprises:

generating a transaction random sequence number based upon the software

authentication parameters of the authentic payment software; and

generating an encryption key based upon the transaction random sequence number and the PIE.

13. The method of claim 12, wherein the generating of the encryption key further comprises:

generating a current time stamp;

converting the current time stamp to a string;

using a one way function to convert the current time stamp string to a current time stamp value;

determining a time difference value between the current time stamp and the initialization time stamp;

computing a Keyed-Hashing for Message Authentication (HMAC) result, based upon the initialization random seed number and the time difference value, to generate the transaction random sequence number;

selecting a number of bits from the HMAC result as the transaction random sequence number and combining the selected number of bits with the PIE;

computing a hash value of the combination; and

selecting a number of bits of the hash value to generate the encryption key.

14. The method of claim 13, wherein the number of bits is about 128.

15. The method of claim 4, wherein an online payment system provides the mobile phone cashless monetary transaction activation link to a member of the online payment system as the user, thereby providing person-to-person mobile phone authenticable cashless monetary transactions using the user's mobile phone wireless wallet.

16. The method of claim 15, further comprising:

displaying on the mobile phone of the user a graphical user interface presenting selectable menu items comprising person-to-person payment, person-to-person transaction, a pending payment request by another person, setup, or any combination thereof;

upon selection of the person-to-person payment or the pending payment request menu items, displaying a graphical user interface accepting inputs comprising a mobile phone number, an email address or any combination thereof, of a transaction party; and

upon input of a mobile phone number and/or an email address of the transaction party, and the PIE, executing the mobile phone cashless monetary transaction with the

transaction party using the mobile phone wireless wallet of the mobile phone user.

17. The method of claim 16, wherein the accepting inputs further comprises accepting abstracted previously registered financial account reference identifiers of the mobile phone user to execute the transaction.

18. The method of claim 1,

wherein the mobile phone authenticable cashless monetary transaction is performed according to Universal Pervasive Transaction Framework Secure Agreement Submission (UPTF SAS) protocol, and the method further comprises:

correlating, at the STS, abstracted financial entity information of the user with the authentic mobile payment software; and

providing person-to-person mobile phone UPTF authenticable cashless monetary transactions using the user mobile phone wireless wallet.

19. The method of claim 1, wherein the PIE is an alphanumeric string having less than or equal to 5 characters.

20. The method of claim 6, further comprising transmitting the mobile phone authenticable cashless transaction messages over a mobile phone communications network according to Hypertext Transfer Protocol (HTTP), socket based communication, and/or web service calls.

21. The method of claim 8, wherein the executing of the mobile phone cashless monetary transaction further comprises:

receiving a mobile phone display screen displayable barcode image as a receipt of the executed mobile phone cashless monetary transaction and/or other transaction, receipt related information;

displaying the barcode image on a display screen of the mobile phone; and

reading, at a physical point of service of the transaction party, the displayed barcode image for transaction management by the transaction party.

22. The method of claim 18, wherein the person-to-person mobile phone UPTF authenticable cashless monetary transactions comprise sending a payment to a person, requesting a payment from another person, checking a pending request for payment from another, storing and retrieving records of transactions, or any combination thereof.

23. The method of claim 1, wherein the installing of the authentic mobile payment software in the mobile phone comprises downloading the authentic mobile payment software to the mobile phone, storing the authentic mobile payment software on a mobile phone installable computer readable medium, storing the authentic mobile payment software in a mobile phone embedded computer readable medium, or any combination thereof.

24. The method of claim 7, wherein the providing of the PIE to the user comprises delivering the PIE to the user as an image through a third party.

25. The method of claim 21, further comprising storing in the mobile phone the barcode image transaction receipt.

26. The method of claim 1, further comprising rewarding a mobile phone wireless wallet transaction with an automatic download of a mobile phone content comprising a ringtone, a game, a digital/media content, software, or any combination thereof, and/or a credit towards any thereof.

27. The method of claim 22, further comprising notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message.

28. The method of claim 21, further comprising notifying the user at the mobile phone of a status of the mobile phone UPTF authenticable cashless monetary transaction using Short/Multimedia Message Service, email, and/or voice message, including transaction receipt information.

29. The method of claim 18, wherein the PIE is an alphanumeric string having less than or equal to 5 characters.

30. A mobile phone, comprising:

a computer readable medium storing a mobile payment software initialized at a secured transaction server (STS) with a software authentication parameter and correlated with a personal identification entry (PIE), as an authentic mobile payment software; and

a programmed computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising:

prompting a user to input the PIE, and

generating according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction over a mobile phone network, as a mobile phone wireless wallet of the user of the mobile phone.

31. A computer system, comprising:

a computer server comprising a programmed computer controlling the server according to a process comprising:

initializing a mobile payment software with a software authentication parameter, as an authentic mobile payment software,

generating a secured personal identification entry (PIE);

providing a secured correlation between the PIE and the authentic mobile payment software, and

providing an online purchasing interface; and

a mobile phone in mobile phone network communication with the server and comprising:

a computer readable medium storing the authentic mobile payment software, and

a computer processor executing the authentic mobile payment software controlling the mobile phone according to a process comprising:

interfacing with the online purchasing interface to generate a virtual shopping cart,

prompting a user to input the PIE,

generating according to the PIE and the software authentication parameter a transformed secure authenticable mobile phone cashless monetary transaction based upon the virtual shopping cart, and

transmitting over the mobile phone network the transformed secure authenticable mobile phone cashless monetary transaction to the computer server to execute the transaction.

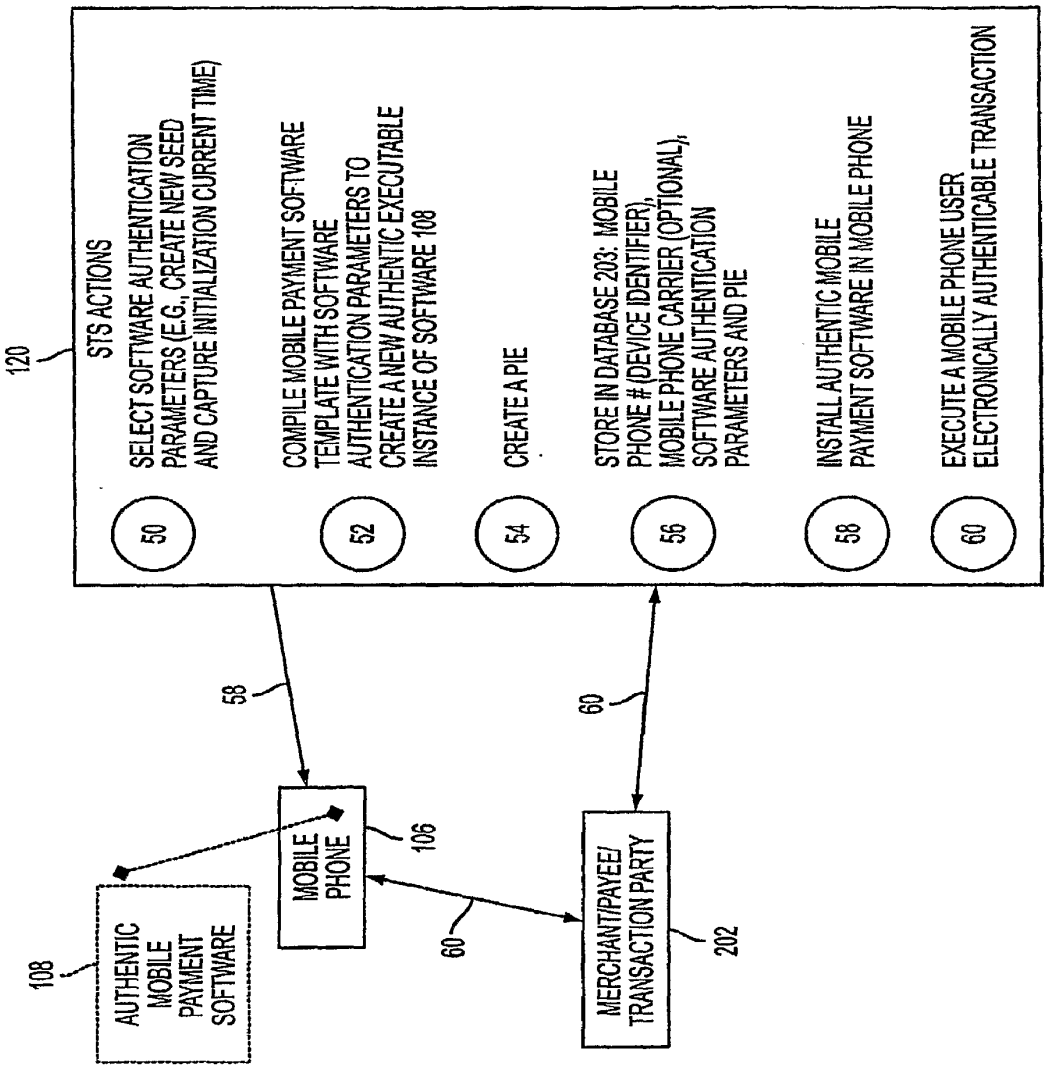

120
STS ACTIONS
50
SELECT SOFTWARE AUTHENTICATION PARAMETERS (E.G., CREATE NEW SEED AND CAPTURE INITIALIZATION CURRENT TIME)
52
COMPILE MOBILE PAYMENT SOFTWARE TEMPLATE WITH SOFTWARE AUTHENTICATION PARAMETERS TO CREATE A NEW AUTHENTIC EXECUTABLE INSTANCE OF SOFTWARE 108
54
CREATE A PIE
56
STORE IN DATABASE 203: MOBILE PHONE # (DEVICE IDENTIFIER), MOBILE PHONE CARRIER (OPTIONAL), SOFTWARE AUTHENTICATION PARAMETERS AND PIE
58
INSTALL AUTHENTIC MOBILE PAYMENT SOFTWARE IN MOBILE PHONE
60
EXECUTE A MOBILE PHONE USER ELECTRONICALLY AUTHENTICABLE TRANSACTION
58
60
MOBILE PHONE
106
AUTHENTIC MOBILE PAYMENT SOFTWARE
108
60
MERCHANT/PAYEE/ TRANSACTION PARTY
202

FIG. 1A

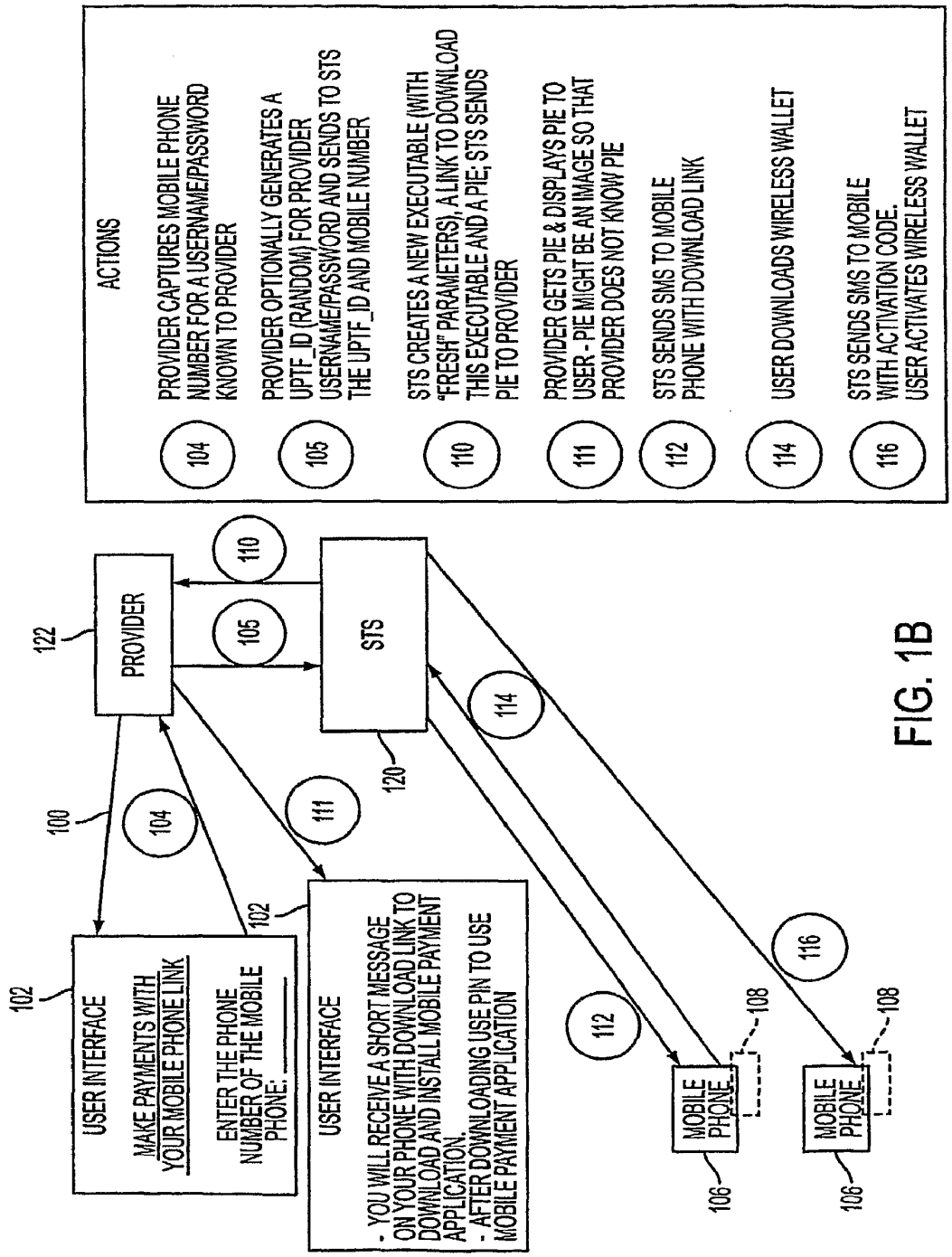

ACTIONS
104 PROVIDER CAPTURES MOBILE PHONE NUMBER FOR A USERNAME/PASSWORD KNOWN TO PROVIDER
105 PROVIDER OPTIONALLY GENERATES A UPTF_ID (RANDOM) FOR PROVIDER USERNAME/PASSWORD AND SENDS TO STS THE UPTF_ID AND MOBILE NUMBER
110 STS CREATES A NEW EXECUTABLE (WITH "FRESH" PARAMETERS), A LINK TO DOWNLOAD THIS EXECUTABLE AND A PIE; STS SENDS PIE TO PROVIDER
111 PROVIDER GETS PIE & DISPLAYS PIE TO USER - PIE MIGHT BE AN IMAGE SO THAT PROVIDER DOES NOT KNOW PIE
112 STS SENDS SMS TO MOBILE PHONE WITH DOWNLOAD LINK
114 USER DOWNLOADS WIRELESS WALLET
116 STS SENDS SMS TO MOBILE WITH ACTIVATION CODE. USER ACTIVATES WIRELESS WALLET
PROVIDER
STS
USER INTERFACE
MAKE PAYMENTS WITH YOUR MOBILE PHONE LINK
ENTER THE PHONE NUMBER OF THE MOBILE PHONE: ____
USER INTERFACE
- YOU WILL RECEIVE A SHORT MESSAGE ON YOUR PHONE WITH DOWNLOAD LINK TO DOWNLOAD AND INSTALL MOBILE PAYMENT APPLICATION.
- AFTER DOWNLOADING USE PIN TO USE MOBILE PAYMENT APPLICATION
MOBILE PHONE
MOBILE PHONE
100
102
102
120
122
106
106
108
108

FIG. 1B

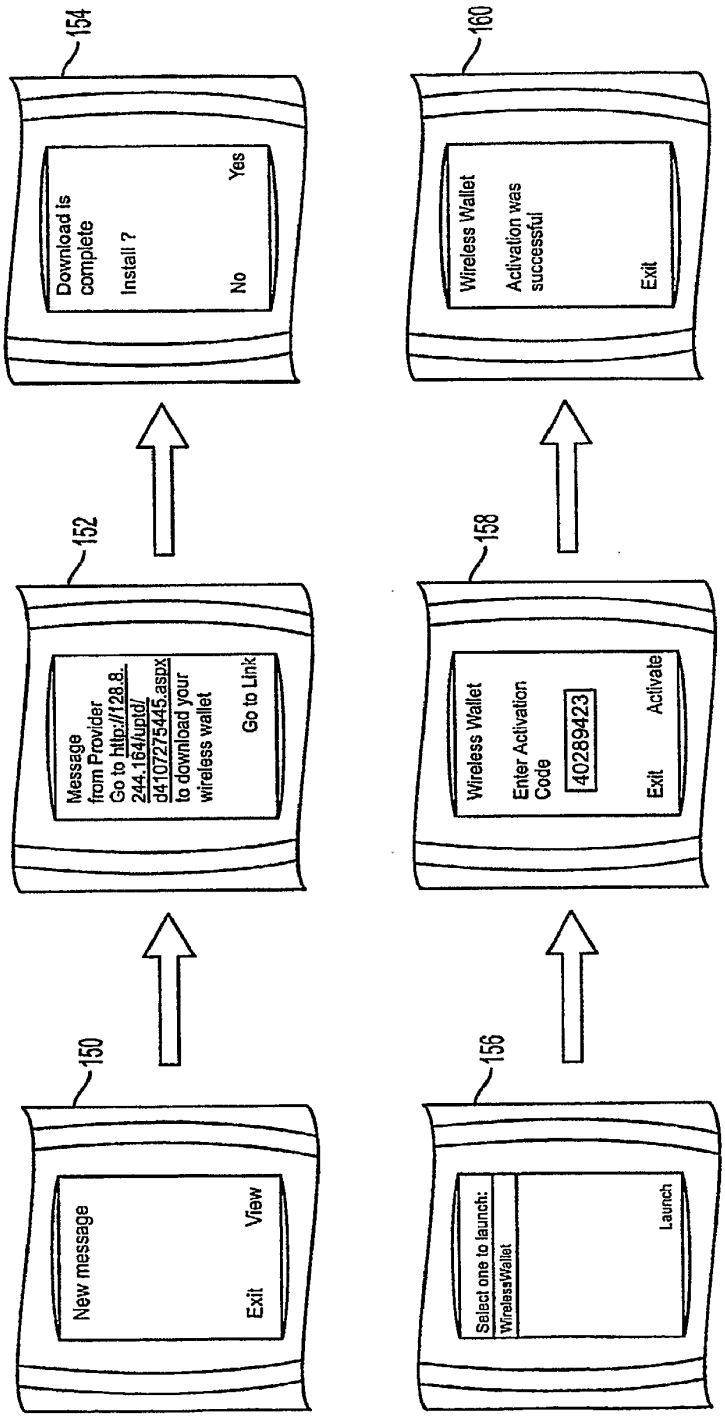

154
Download is complete
Install ?
Yes
No
160
Wireless Wallet
Activation was successful
Exit
152
Message from Provider
Go to http://128.8.244.164/uptd/d4107275445.aspx to download your wireless wallet
Go to Link
158
Wireless Wallet
Enter Activation Code
40289423
Exit
Activate
150
New message
Exit
View
156
Select one to launch:
WirelessWallet
Launch

FIG. 1C

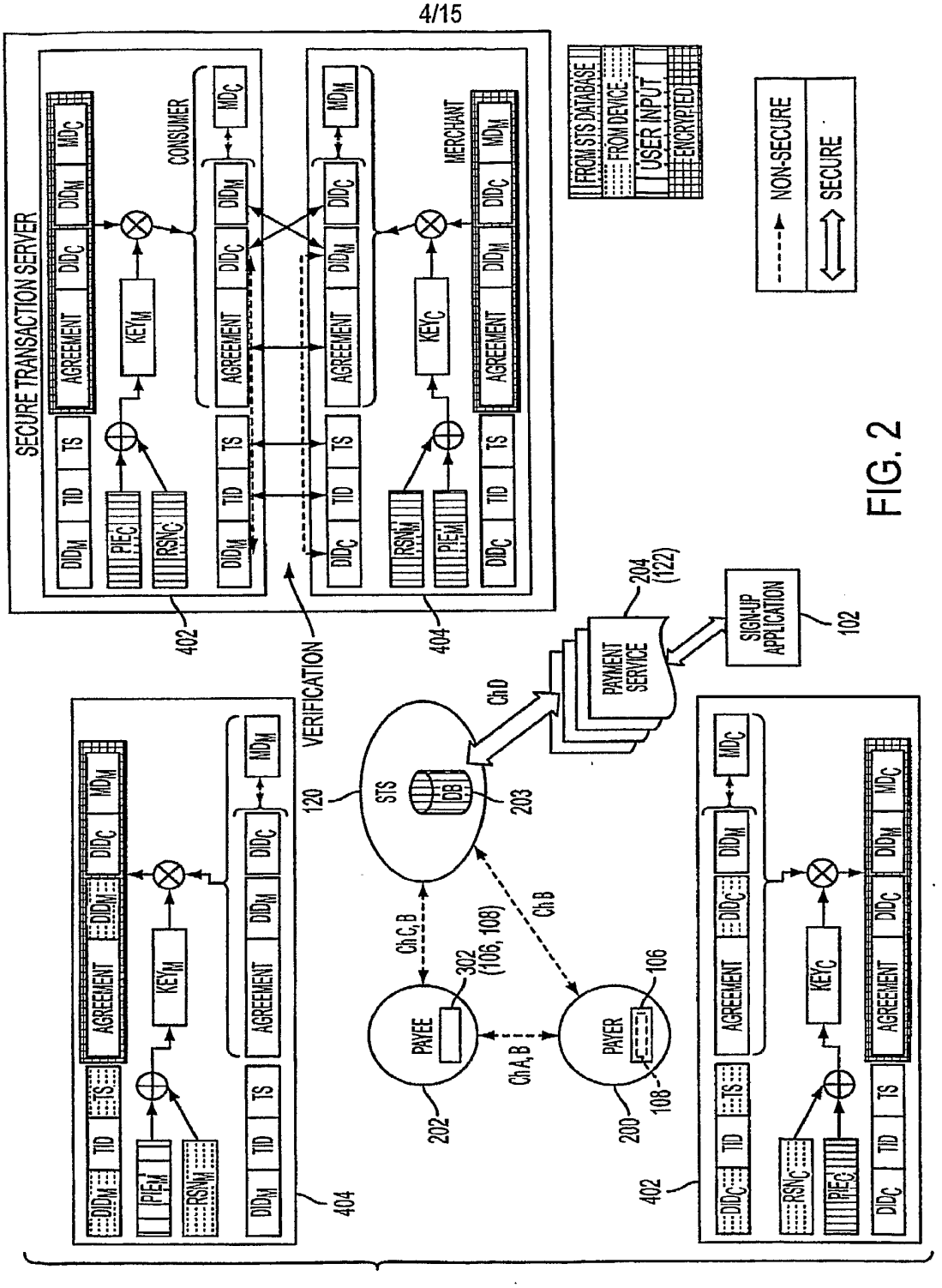

SECURE TRANSACTION SERVER
CONSUMER
MERCHANT
AGREEMENT
KEYM
KEYC
PIEC
RSNC
PIEM
RSNM
DIDM
DIDC
MDM
MDC
TID
TS
FROM STS DATABASE
FROM DEVICE
USER INPUT
ENCRYPTED
NON-SECURE
SECURE
402
404
VERIFICATION
120
STS
DB
203
ChD
PAYMENT SERVICE
204 (122)
SIGN-UP APPLICATION
102
ChC,B
302 (106, 108)
ChB
ChA,B
PAYEE
PAYER
202
200
106
108

FIG. 2

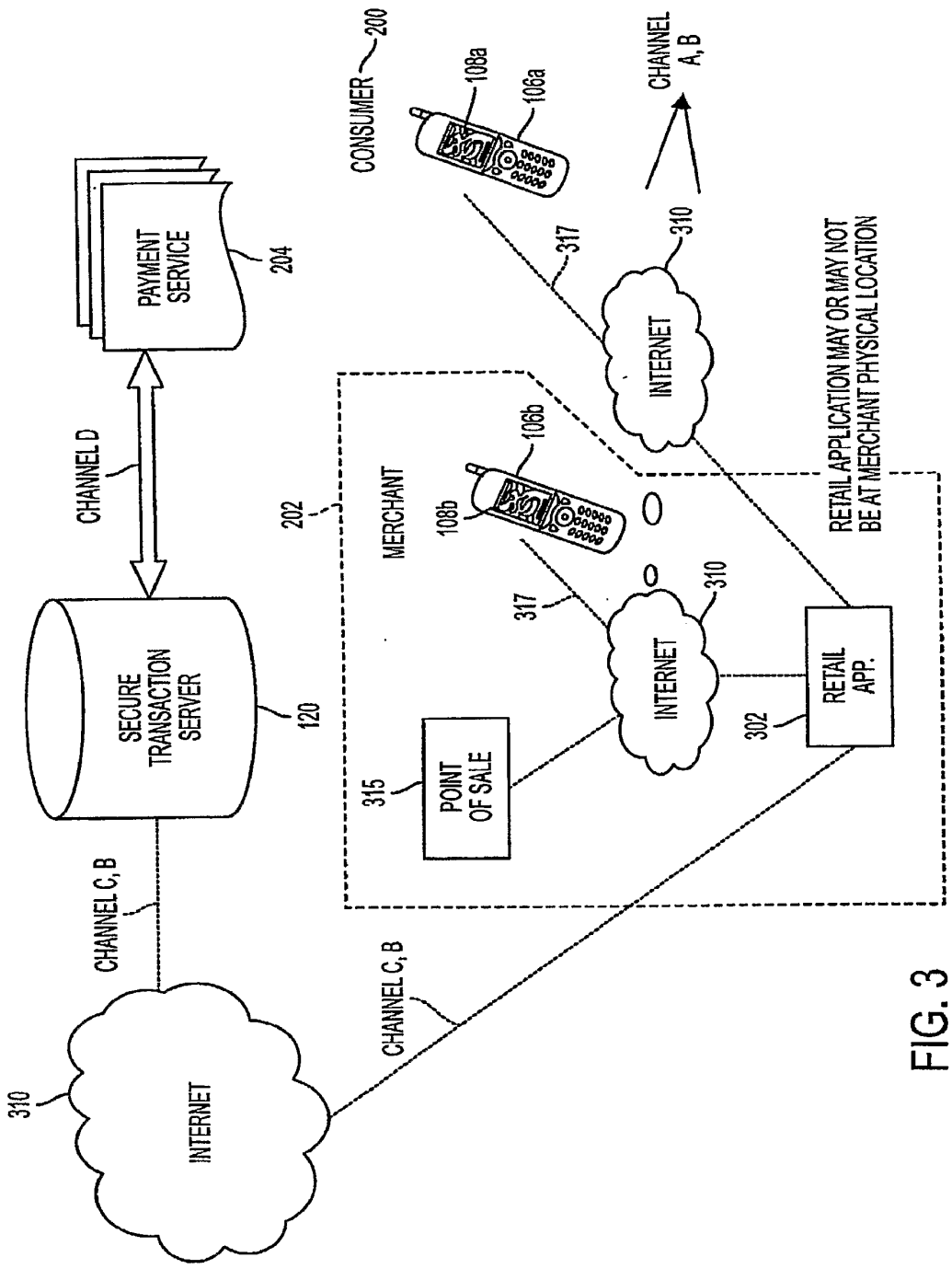
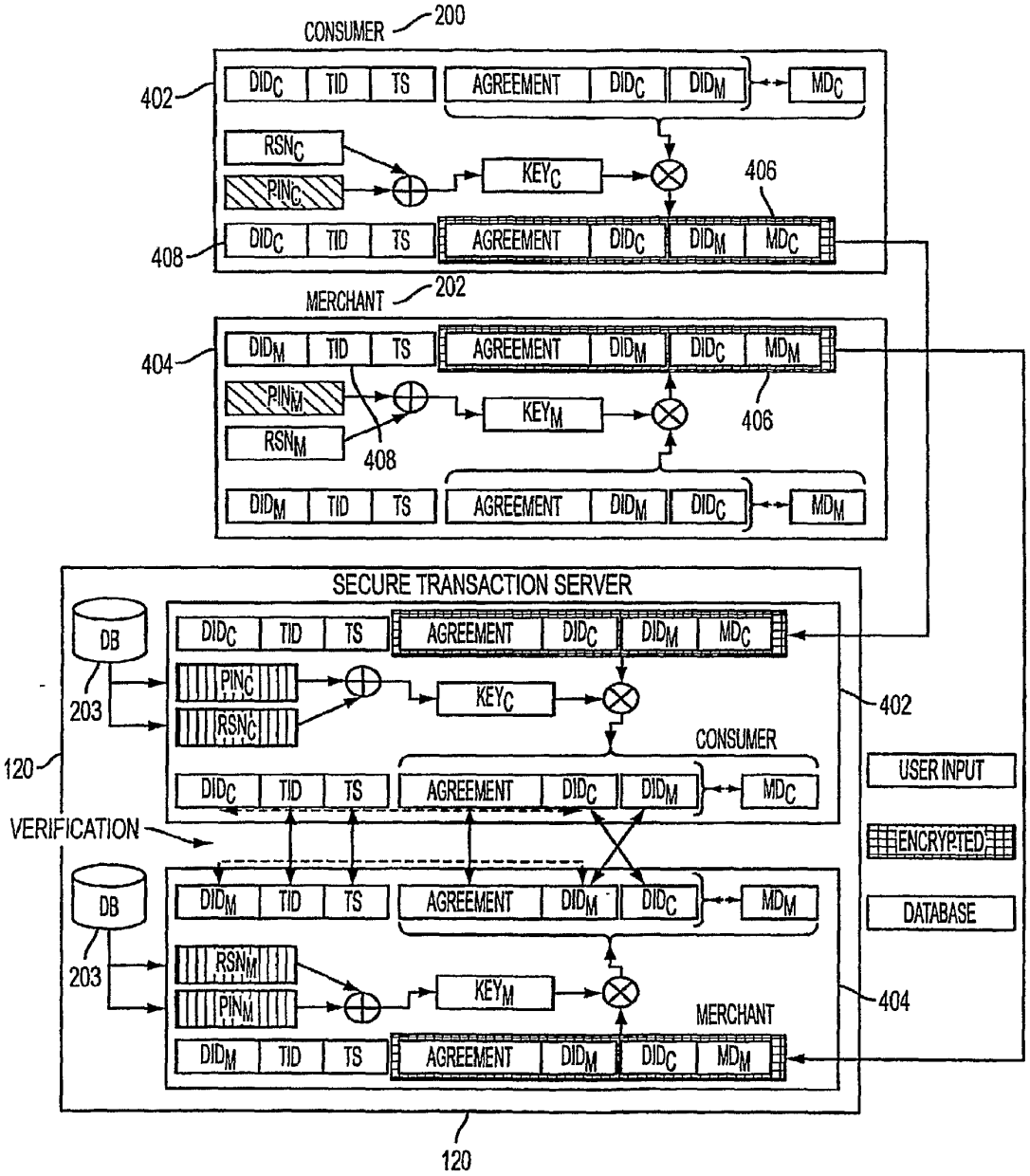

CONSUMER
200
108a
106a
CHANNEL A, B
PAYMENT SERVICE
204
317
310
INTERNET
CHANNEL D
106b
MERCHANT
202
108b
RETAIL APPLICATION MAY OR MAY NOT BE AT MERCHANT PHYSICAL LOCATION
317
310
INTERNET
RETAIL APP.
302
SECURE TRANSACTION SERVER
120
315
POINT OF SALE
CHANNEL C, B
CHANNEL C, B
310
INTERNET

FIG. 3



CONSUMER AND MERCHANT MESSAGE ENCRYPTION AND SECURE TRANSACTION SERVER PROCESSING

FIG. 4

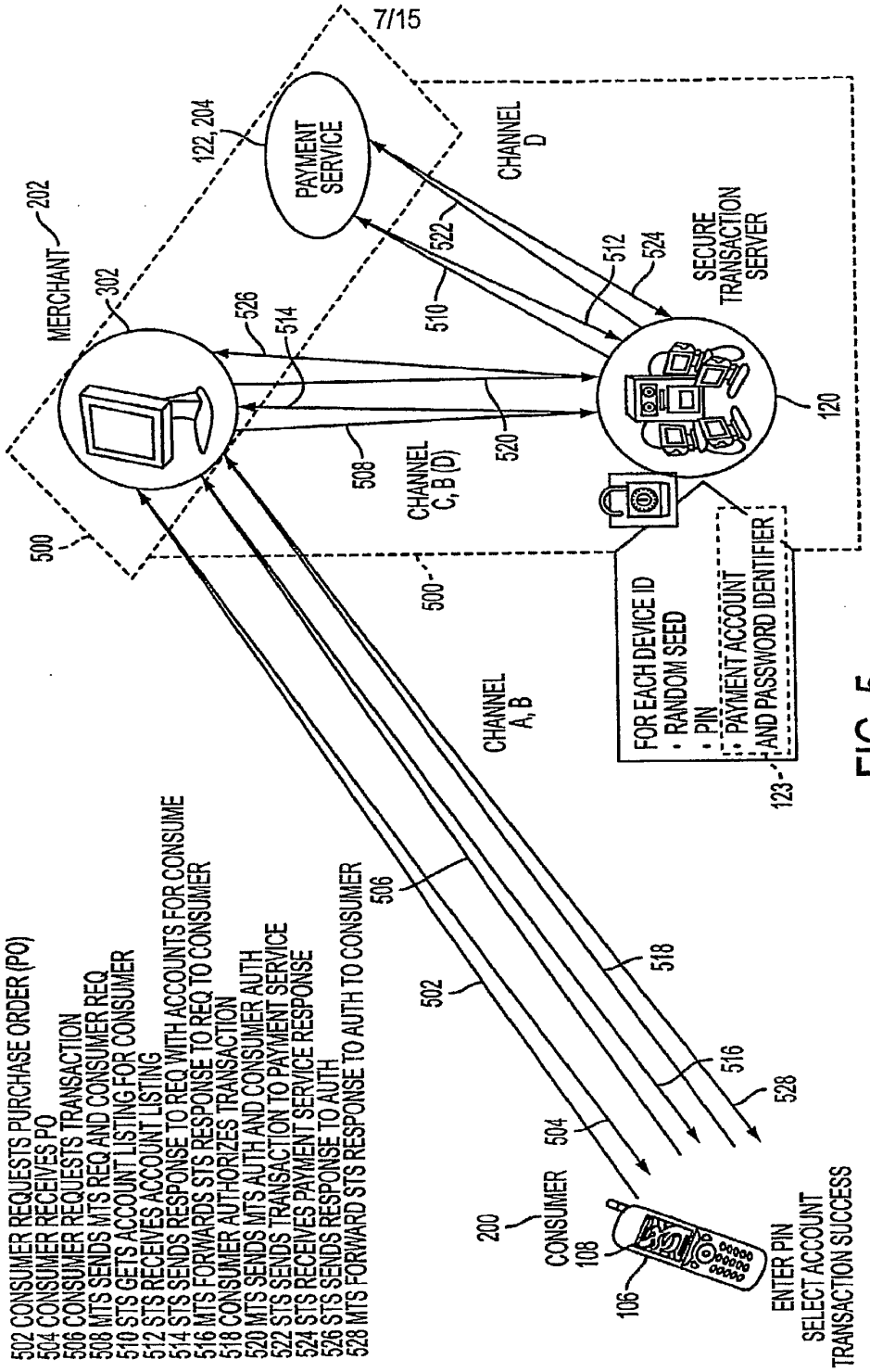

A COMPLETE TRANSACTION
502 CONSUMER REQUESTS PURCHASE ORDER (PO)
504 CONSUMER RECEIVES PO
506 CONSUMER REQUESTS TRANSACTION
508 MTS SENDS MTS REQ AND CONSUMER REQ
510 STS GETS ACCOUNT LISTING FOR CONSUMER
512 STS RECEIVES ACCOUNT LISTING
514 STS SENDS RESPONSE TO REQ WITH ACCOUNTS FOR CONSUME
516 MTS FORWARDS STS RESPONSE TO REQ TO CONSUMER
518 CONSUMER AUTHORIZES TRANSACTION
520 MTS SENDS MTS AUTH AND CONSUMER AUTH
522 STS SENDS TRANSACTION TO PAYMENT SERVICE
524 STS RECEIVES PAYMENT SERVICE RESPONSE
526 STS SENDS RESPONSE TO AUTH
528 MTS FORWARD STS RESPONSE TO AUTH TO CONSUMER
MERCHANT
202
302
500
122, 204
PAYMENT SERVICE
CHANNEL D
SECURE TRANSACTION SERVER
120
CHANNEL C, B (D)
CHANNEL A, B
FOR EACH DEVICE ID
• RANDOM SEED
• PIN
• PAYMENT ACCOUNT
AND PASSWORD IDENTIFIER
123
CONSUMER
200
108
106
ENTER PIN
SELECT ACCOUNT
TRANSACTION SUCCESS

FIG. 5

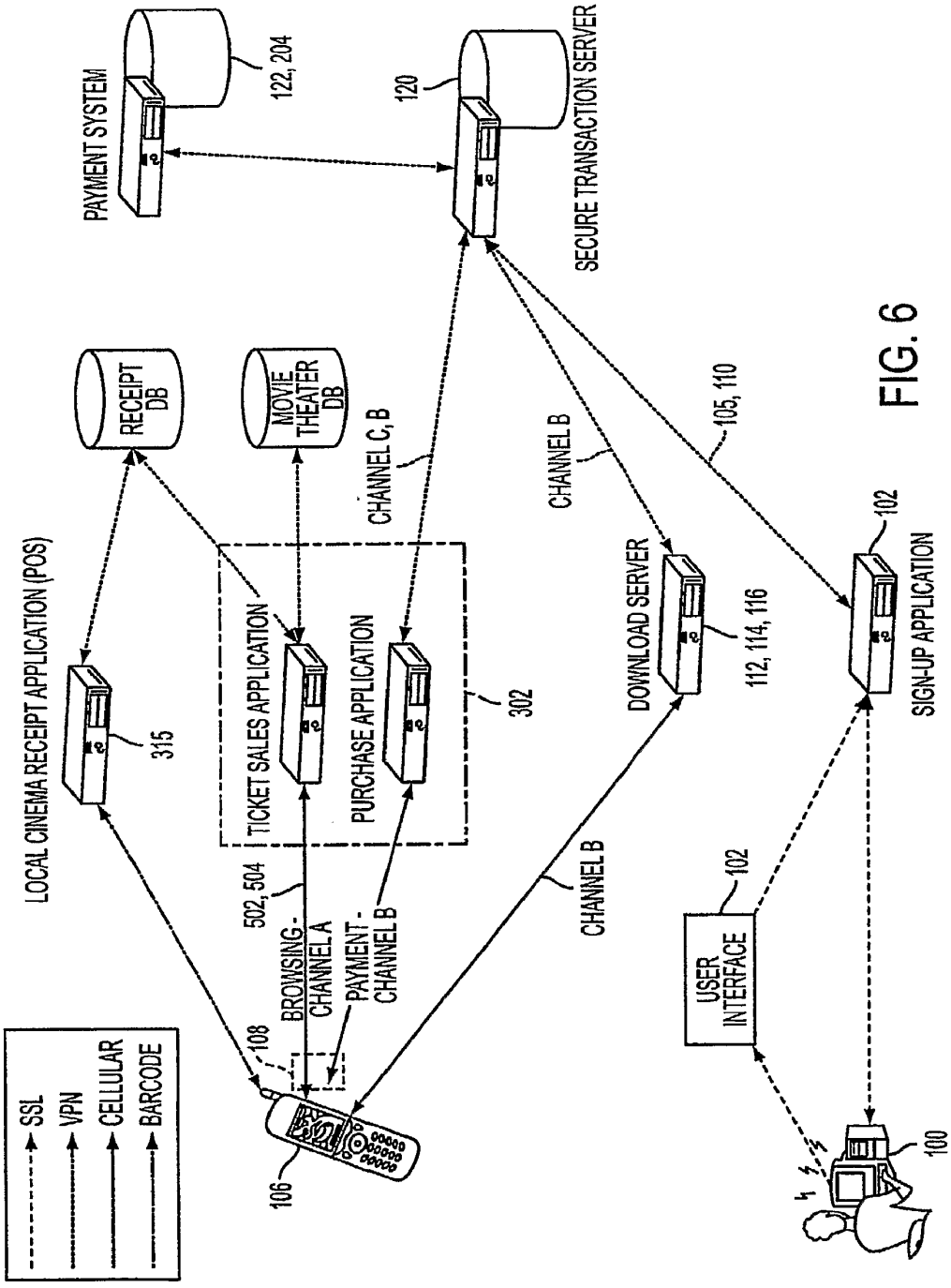

PAYMENT SYSTEM
122, 204
120
SECURE TRANSACTION SERVER
RECEIPT DB
MOVIE THEATER DB
CHANNEL C, B
CHANNEL B
105, 110
LOCAL CINEMA RECEIPT APPLICATION (POS)
315
TICKET SALES APPLICATION
PURCHASE APPLICATION
302
DOWNLOAD SERVER
112, 114, 116
102
SIGN-UP APPLICATION
502, 504
BROWSING - CHANNEL A
PAYMENT - CHANNEL B
CHANNEL B
USER INTERFACE
102
108
106
100
SSL
VPN
CELLULAR
BARCODE

FIG. 6

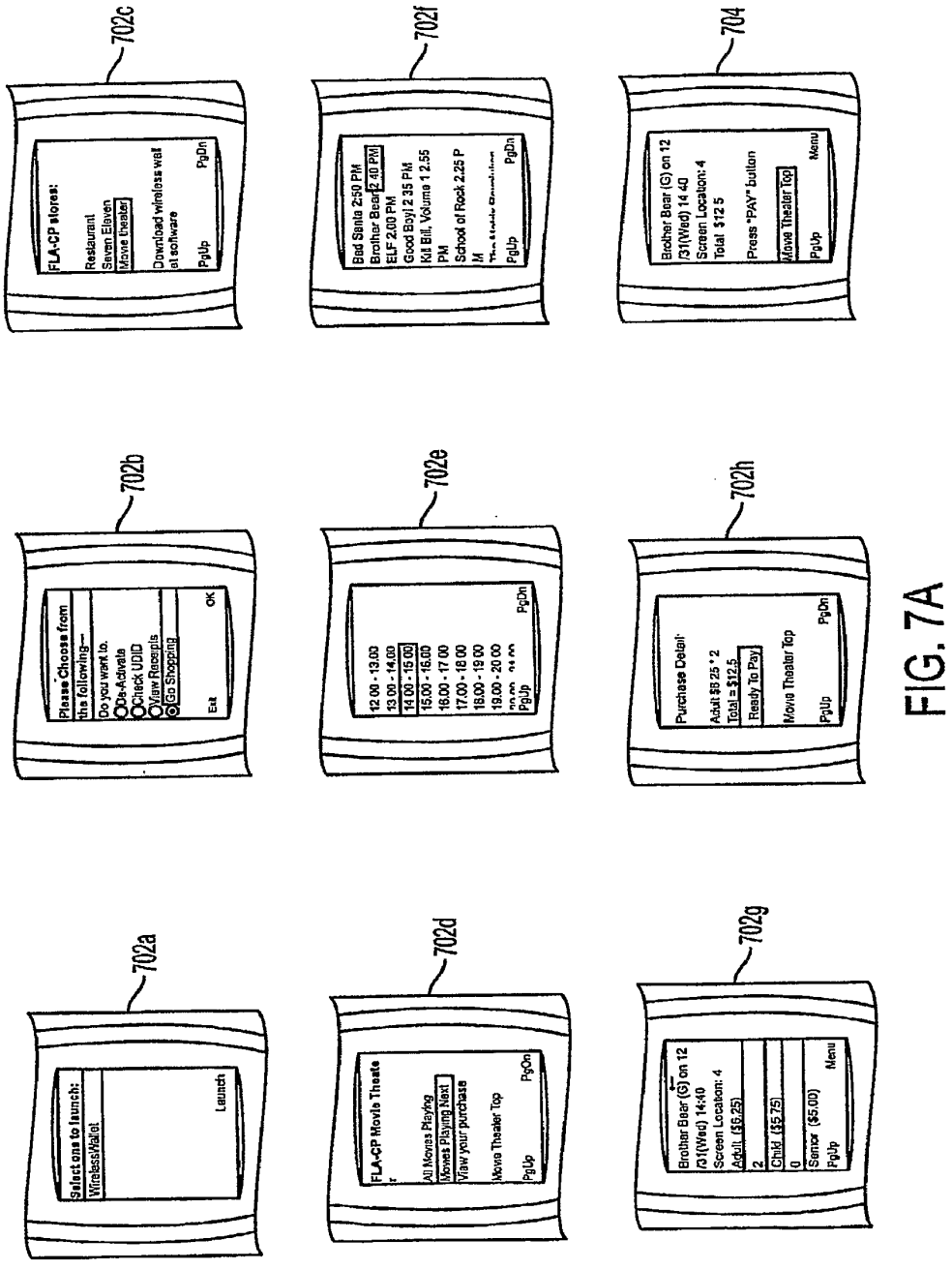

702c
FLA-CP stores:
Restaurant
Seven Eleven
Movie theater
Download wireless wall st software
PgUp
PgDn
702f
Bad Santa 2:50 PM
Brother Bear 2:40 PM
ELF 2:00 PM
Good Boy! 2:35 PM
Kill Bill, Volume 1 2:55 PM
School of Rock 2:25 P M
PgUp
PgDn
704
Brother Bear (G) on 12 /31(Wed) 14:40
Screen Location: 4
Total $12.5
Press "PAY" button
Movie Theater Top
Menu
PgUp
702b
Please Choose from the following—
Do you want to:
De-Activate
Check UDID
View Receipts
Go Shopping
OK
Exit
702e
12:00 - 13:00
13:00 - 14:00
14:00 - 15:00
15:00 - 16:00
16:00 - 17:00
17:00 - 18:00
18:00 - 19:00
19:00 - 20:00
PgUp
PgDn
702h
Purchase Detail
Adult $8.25 * 2
Total = $12.5
Ready To Pay
Movie Theater Top
PgUp
PgDn
702a
Select one to launch:
WirelessWallet
Launch
702d
FLA-CP Movie Theate
All Movies Playing
Movies Playing Next
View your purchase
Movie Theater Top
PgUp
PgDn
702g
Brother Bear (G) on 12 /31(Wed) 14:40
Screen Location: 4
Adult ($8.25)
2
Child ($5.75)
0
Senior ($5.00)
PgUp
Menu

FIG. 7A

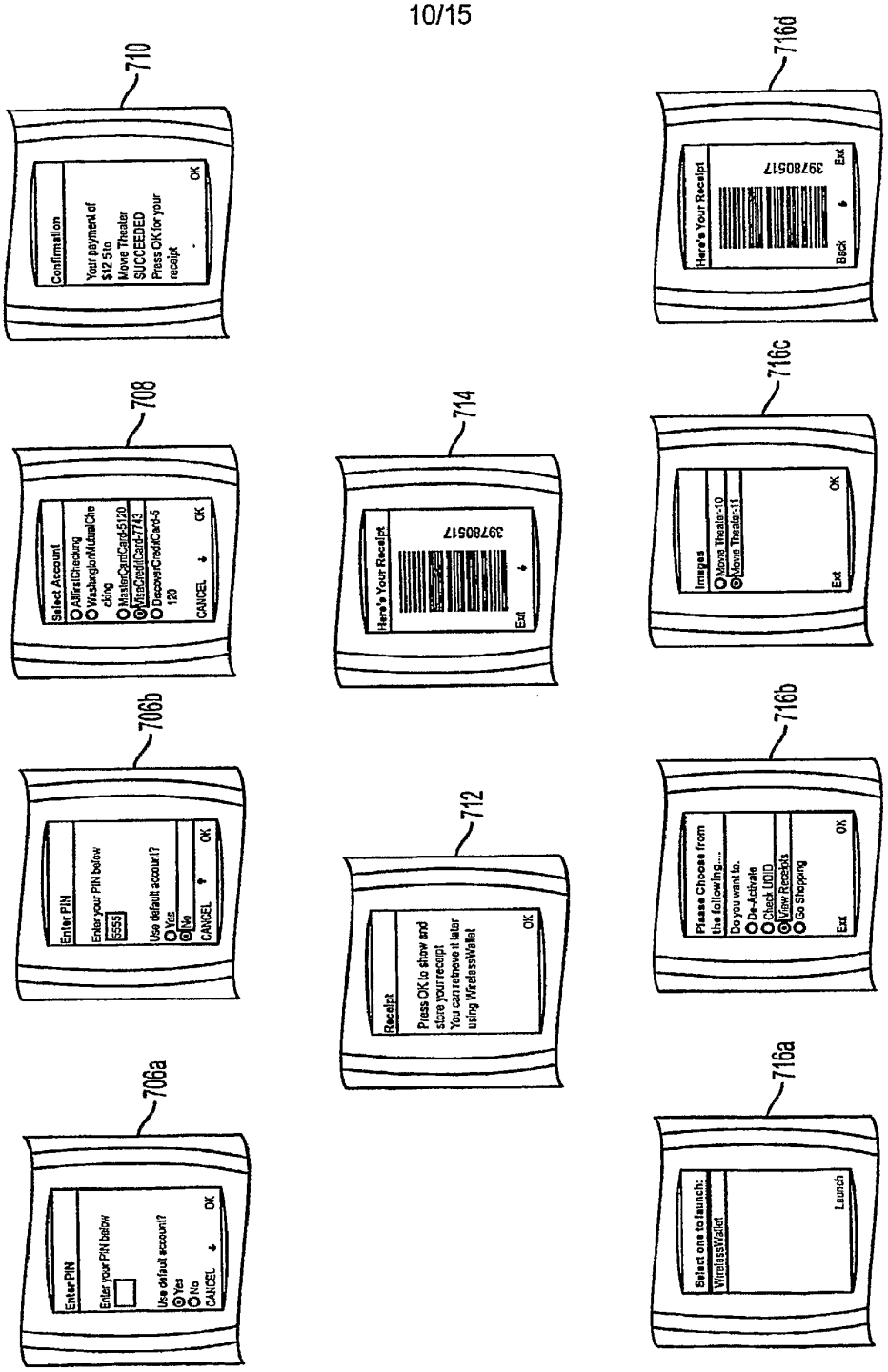

710
Confirmation
Your payment of
$12.5 to
Move Theater
SUCCEEDED
Press OK for your
receipt
OK
716d
Here's Your Receipt
39780517
Back
Ext
708
Select Account
AlliraCheckng
WashingtonMutualChe
cking
MasterCardCard-5120
MiteCreditCard-7743
DiscoverCreditCard-5
120
CANCEL
OK
714
Here's Your Receipt
39780517
Ext
716c
Images
Mona Theater-10
Mona Theater-11
OK
Ext
706b
Enter PIN
Enter your PIN below
5555
Use default account?
Yes
No
CANCEL
OK
712
Receipt
Press OK to show and
store your receipt
You can retrieve it later
using WirelessWallet
OK
716b
Please Choose from
the following....
Do you want to.
De-Activate
Check UOID
View Receipts
Go Shopping
OK
Ext
706a
Enter PIN
Enter your PIN below
Use default account?
Yes
No
CANCEL
OK
716a
Select one to launch:
WirelessWallet
Launch

FIG. 7B

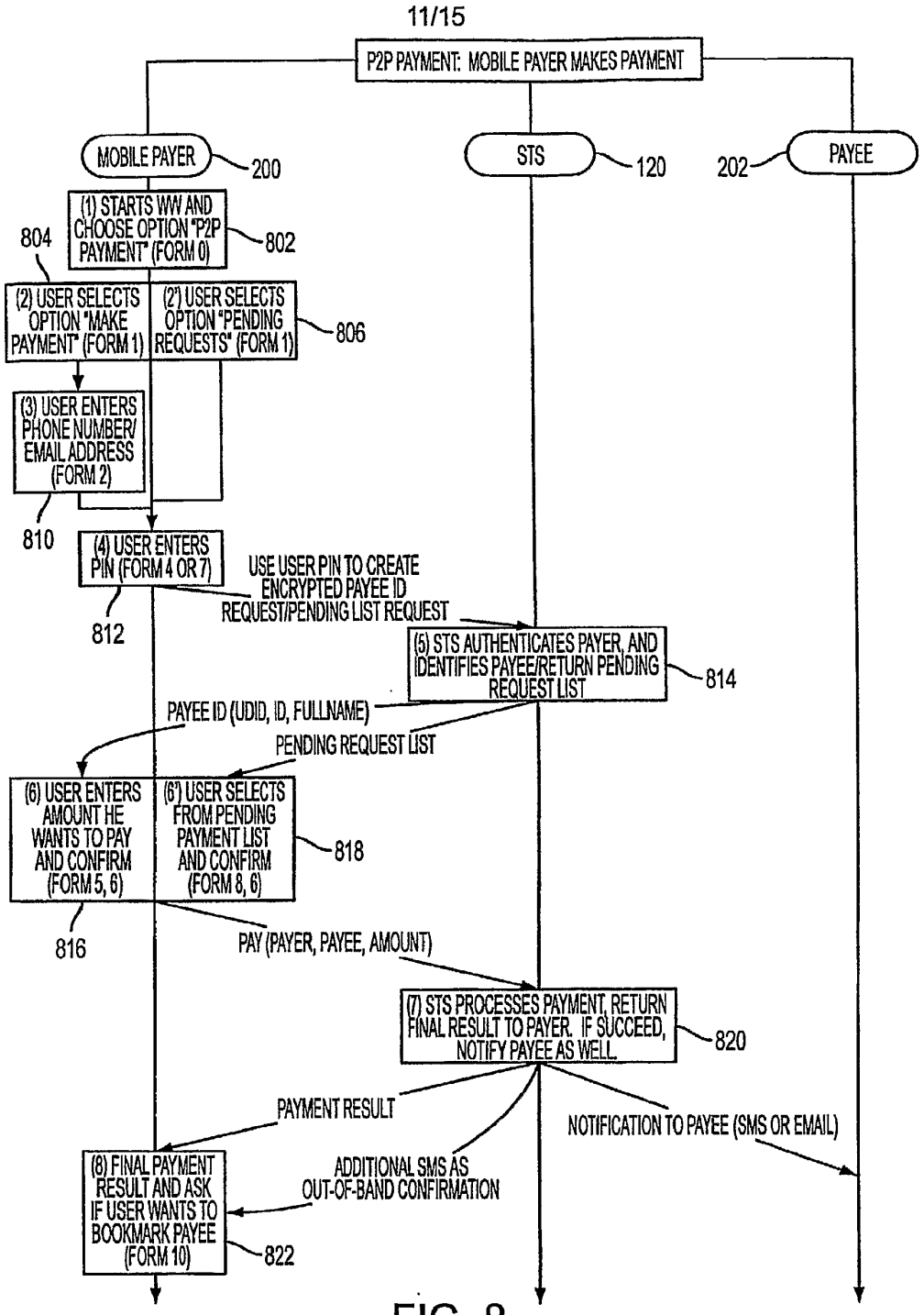

P2P PAYMENT: MOBILE PAYER MAKES PAYMENT
MOBILE PAYER
200
STS
120
202
PAYEE
(1) STARTS WW AND CHOOSE OPTION "P2P PAYMENT" (FORM 0)
802
804
(2) USER SELECTS OPTION "MAKE PAYMENT" (FORM 1)
(2') USER SELECTS OPTION "PENDING REQUESTS" (FORM 1)
806
(3) USER ENTERS PHONE NUMBER/ EMAIL ADDRESS (FORM 2)
810
(4) USER ENTERS PIN (FORM 4 OR 7)
812
USE USER PIN TO CREATE ENCRYPTED PAYEE ID REQUEST/PENDING LIST REQUEST
(5) STS AUTHENTICATES PAYER, AND IDENTIFIES PAYEE/RETURN PENDING REQUEST LIST
814
PAYEE ID (UDID, ID, FULLNAME)
PENDING REQUEST LIST
(6) USER ENTERS AMOUNT HE WANTS TO PAY AND CONFIRM (FORM 5, 6)
(6') USER SELECTS FROM PENDING PAYMENT LIST AND CONFIRM (FORM 8, 6)
818
816
PAY (PAYER, PAYEE, AMOUNT)
(7) STS PROCESSES PAYMENT, RETURN FINAL RESULT TO PAYER. IF SUCCEED, NOTIFY PAYEE AS WELL.
820
PAYMENT RESULT
NOTIFICATION TO PAYEE (SMS OR EMAIL)
(8) FINAL PAYMENT RESULT AND ASK IF USER WANTS TO BOOKMARK PAYEE (FORM 10)
822
ADDITIONAL SMS AS OUT-OF-BAND CONFIRMATION

FIG. 8

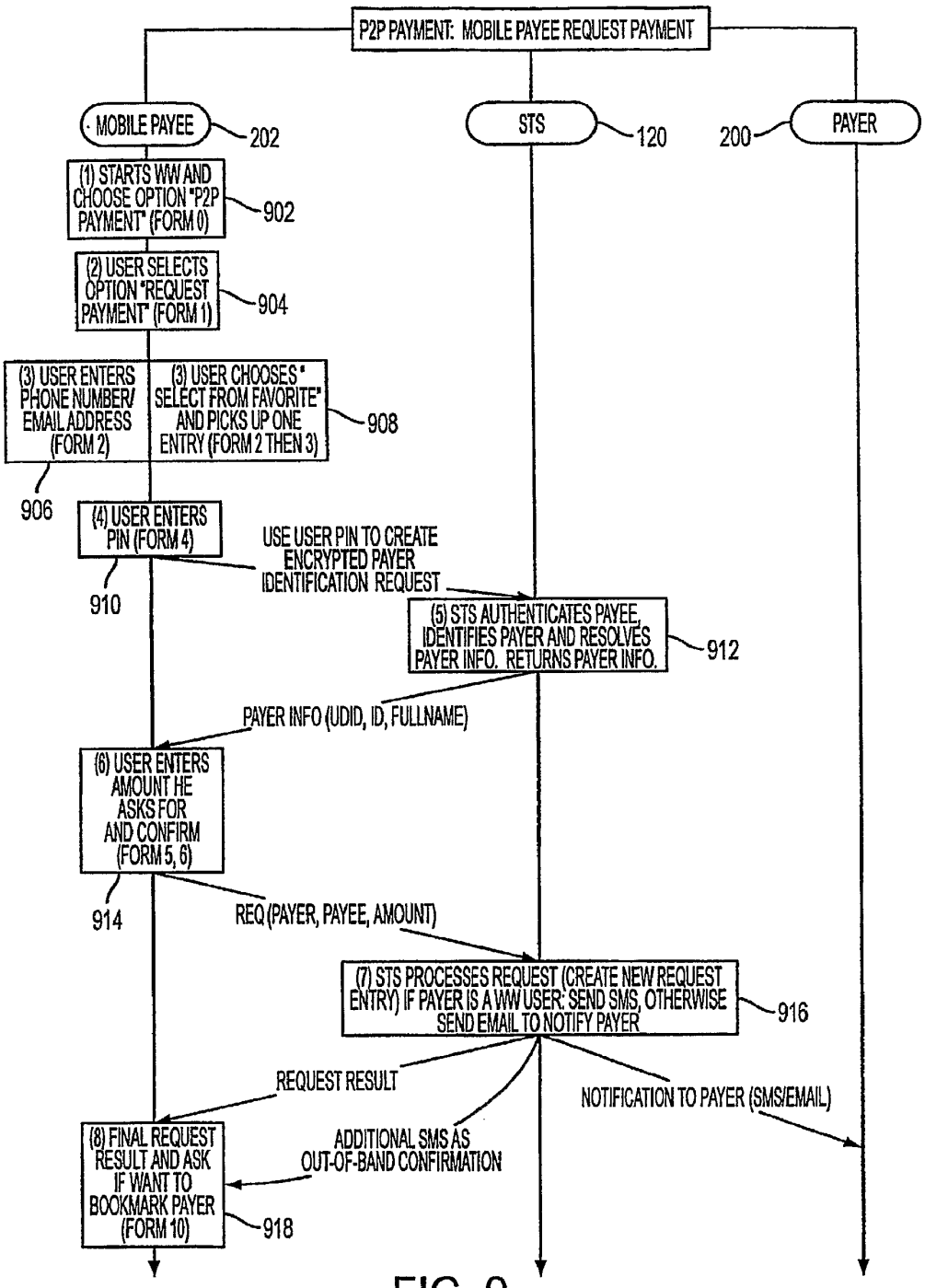

P2P PAYMENT: MOBILE PAYEE REQUEST PAYMENT
MOBILE PAYEE
202
STS
120
200
PAYER
(1) STARTS WW AND CHOOSE OPTION "P2P PAYMENT" (FORM 0)
902
(2) USER SELECTS OPTION "REQUEST PAYMENT" (FORM 1)
904
(3) USER ENTERS PHONE NUMBER/ EMAIL ADDRESS (FORM 2)
(3) USER CHOOSES "SELECT FROM FAVORITE" AND PICKS UP ONE ENTRY (FORM 2 THEN 3)
908
906
(4) USER ENTERS PIN (FORM 4)
910
USE USER PIN TO CREATE ENCRYPTED PAYER IDENTIFICATION REQUEST
(5) STS AUTHENTICATES PAYEE, IDENTIFIES PAYER AND RESOLVES PAYER INFO. RETURNS PAYER INFO.
912
PAYER INFO (UDID, ID, FULLNAME)
(6) USER ENTERS AMOUNT HE ASKS FOR AND CONFIRM (FORM 5, 6)
914
REQ (PAYER, PAYEE, AMOUNT)
(7) STS PROCESSES REQUEST (CREATE NEW REQUEST ENTRY) IF PAYER IS A WW USER: SEND SMS, OTHERWISE SEND EMAIL TO NOTIFY PAYER
916
REQUEST RESULT
NOTIFICATION TO PAYER (SMS/EMAIL)
(8) FINAL REQUEST RESULT AND ASK IF WANT TO BOOKMARK PAYER (FORM 10)
ADDITIONAL SMS AS OUT-OF-BAND CONFIRMATION
918

FIG. 9

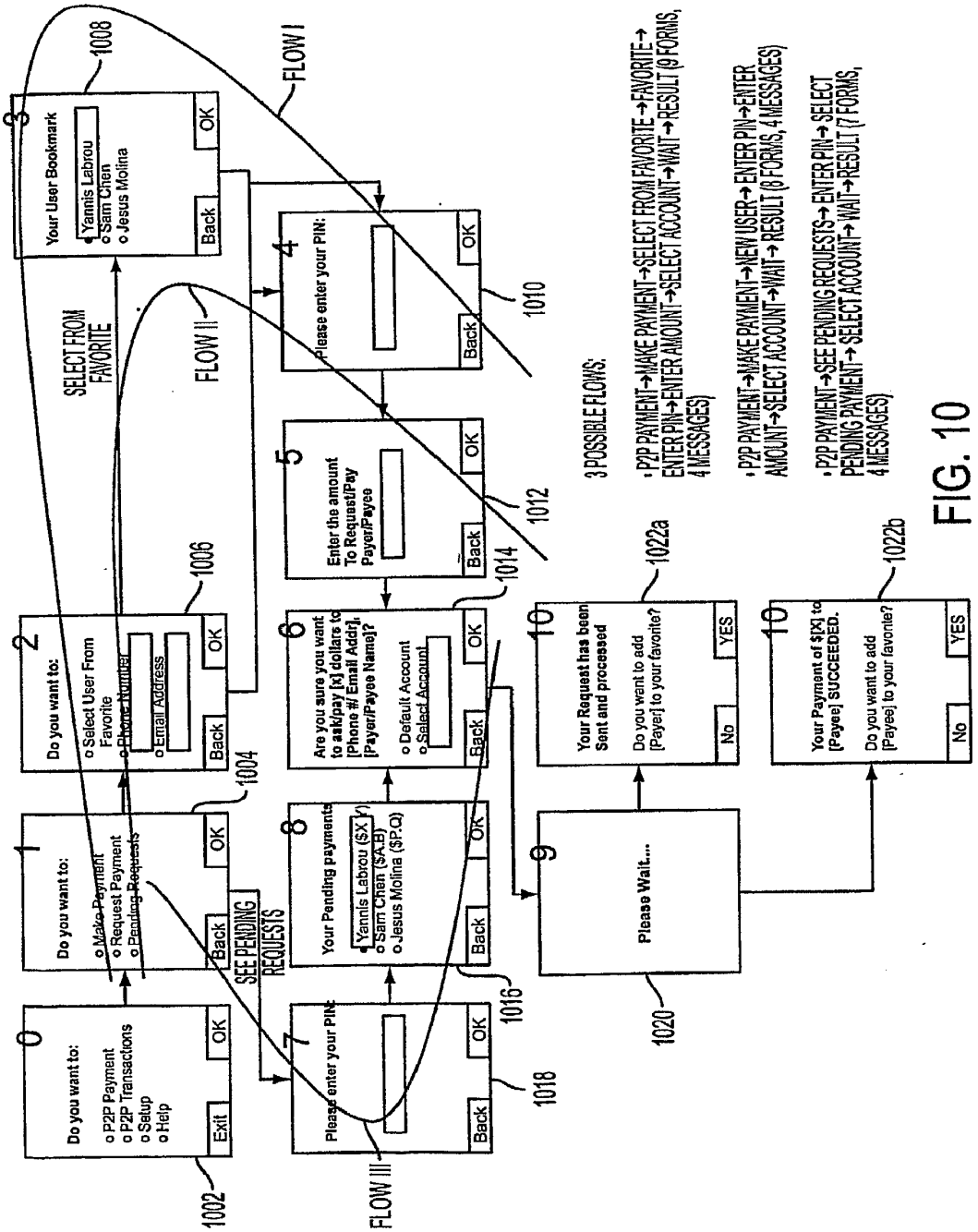

0
Do you want to:
o P2P Payment
o P2P Transactions
o Setup
o Help
Exit
OK
1002
1
Do you want to:
o Make Payment
o Request Payment
o Pending Requests
Back
OK
1004
2
Do you want to:
o Select User From Favorite
o Phone Number
o Email Address
Back
OK
1006
3
Your User Bookmark
Yannis Labrou
Sam Chen
Jesus Molina
Back
OK
1008
4
Please enter your PIN:
Back
OK
1010
5
Enter the amount To Request/Pay Payer/Payee
Back
OK
1012
6
Are you sure you want to ask/pay [x] dollars to [Phone #/ Email Addr], [Payer/Payee Name]?
o Default Account
o Select Account
Back
OK
1014
7
Please enter your PIN:
Back
OK
1016
8
Your Pending payments
Yannis Labrou ($X.Y)
Sam Chen ($A.B)
Jesus Molina ($P.Q)
Back
OK
1018
9
Please Wait...
1020
10
Your Request has been Sent and processed
Do you want to add [Payer] to your favorite?
No
YES
1022a
10
Your Payment of $[X] to [Payee] SUCCEEDED.
Do you want to add [Payee] to your favorite?
No
YES
1022b
SEE PENDING REQUESTS
SELECT FROM FAVORITE
FLOW I
FLOW II
FLOW III
3 POSSIBLE FLOWS:
• P2P PAYMENT→MAKE PAYMENT→SELECT FROM FAVORITE→FAVORITE→ ENTER PIN→ENTER AMOUNT→SELECT ACCOUNT→WAIT→RESULT (9 FORMS, 4 MESSAGES)
• P2P PAYMENT→MAKE PAYMENT→NEW USER→ENTER PIN→ENTER AMOUNT→SELECT ACCOUNT→WAIT→ RESULT (8 FORMS, 4 MESSAGES)
• P2P PAYMENT→SEE PENDING REQUESTS→ ENTER PIN→ SELECT PENDING PAYMENT→ SELECT ACCOUNT→ WAIT→RESULT (7 FORMS, 4 MESSAGES)

FIG. 10

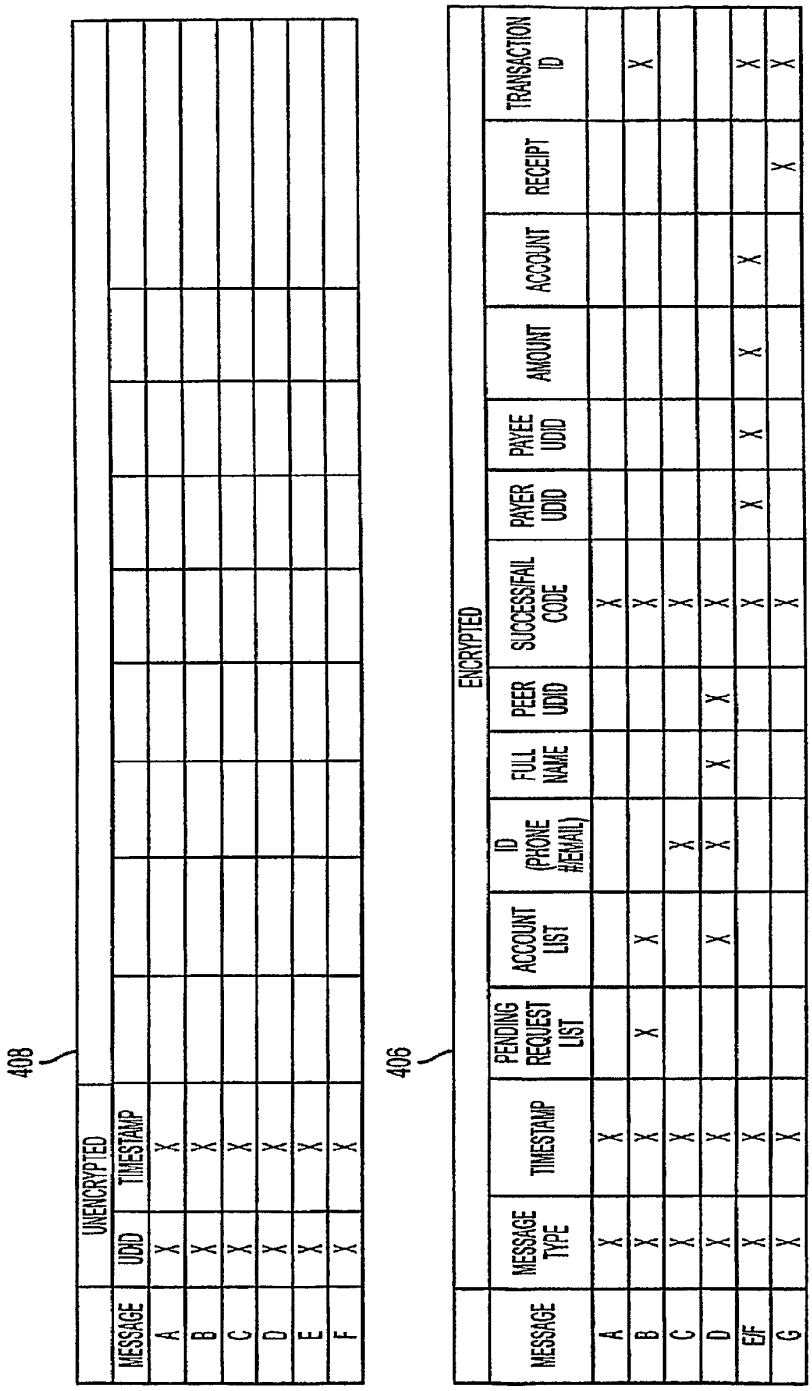

408
UNENCRYPTED
MESSAGE
UDID
TIMESTAMP
A X X
B X X
C X X
D X X
E X X
F X X
406
ENCRYPTED
MESSAGE
MESSAGE TYPE
TIMESTAMP
PENDING REQUEST LIST
ACCOUNT LIST
ID (PHONE #/EMAIL)
FULL NAME
PEER UDID
SUCCESS/FAIL CODE
PAYER UDID
PAYEE UDID
AMOUNT
ACCOUNT
RECEIPT
TRANSACTION ID
A X X X X X
B X X X X X X
C X X X X X
D X X X X X X X X
E/F X X X X X X X
G X X X X X X
MESSAGE A: PENDING REQUEST LIST REQUEST
MESSAGE B: PENDING REQUEST LIST REPLY
MESSAGE C: PEER IDENTIFICATION REQUEST
MESSAGE D: PEER IDENTIFICATION REPLY
MESSAGE E/F: MAKE PAYMENT REQUEST / REQUEST PAYMENT REQUEST
MESSAGE G: TRANSACTION RESULT

FIG. 11

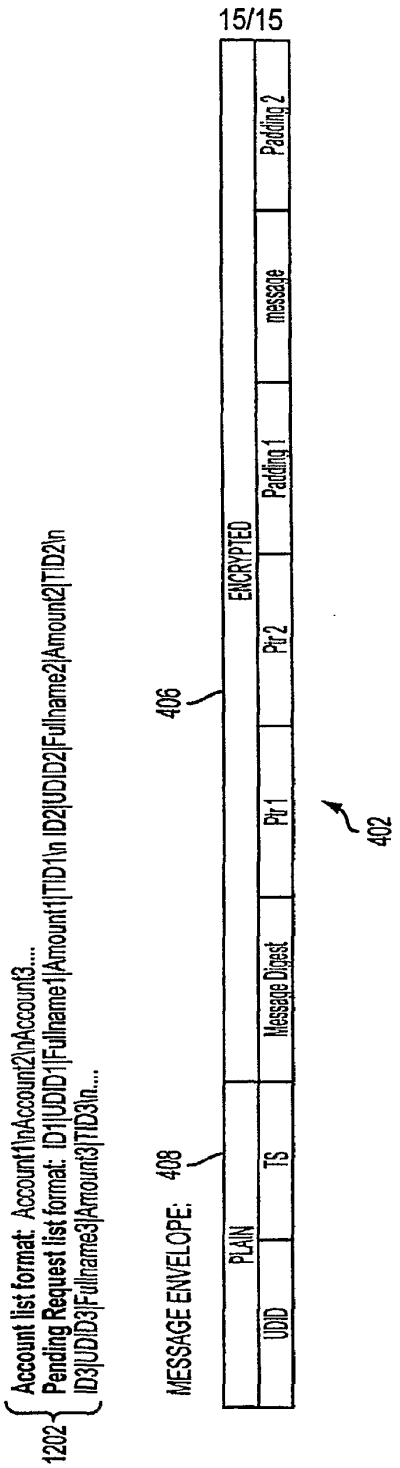

Account list format: Account1\nAccount2\nAccount3....
Pending Request list format: ID1|UDID1|Fullname1|Amount1|TID1\n ID2|UDID2|Fullname2|Amount2|TID2\n ID3|UDID3|Fullname3|Amount3|TID3\n....
1202
MESSAGE ENVELOPE:
408
406
402
UDID
TS
Message Digest
Ptr 1
Ptr 2
Padding 1
message
Padding 2
PLAIN
ENCRYPTED

FIG. 12