accordance with a method wherein digital money is transferred via the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to the figures, preferred and exemplary implementations of the invention will now be described. Initially, techniques of the invention will described with reference to **FIGS. 1 - 5** which illustrate a system employing a mobile telephone wherein signals appropriate for implementing an in-person purchase via a credit or debit account are transmitted between a mobile unit and a merchant cashier register or other point of sale unit via a cellular telephone. The transaction is coordinated by a financial transaction clearinghouse with the financial ID of a credit or debit account selected by the customer being transmitted from the mobile telephone to the clearinghouse, rather than to the merchant cashier register. An alternative method for in-person purchases wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register will be described with reference to **FIG. 6**. Then, alternative systems employing satellite-fleet mobile communications or direct infrared communications between the mobile unit and the merchant cashier register for in-person purchases will be described with reference to **FIGS. 7 - 8**. Next, with reference to **FIGS. 9 - 11**, a system for implementing a purchase wherein the purchaser and merchant are remote from one another will be described both for a credit or debit account purchase and for a digital money purchase. Finally, with reference to **FIGS. 12 - 13** a system for implementing a digital money purchase via the Internet using a lap-top computer with mobile telephony capability will be described.

FIG. 1 shows a system **10** for performing a purchase based upon a credit or debit account between a customer (not shown) using a mobile telephone unit **12** and a merchant (also not shown) using a point of sale cashier register **14**. **FIG. 2** illustrates a method performed by the system of **FIG. 1**. **FIGS. 1** and **2** will be described together with the steps of **FIG. 2** provided in parentheses. After the customer verbally indicates a desire to purchase goods or services, the merchant enters purchase transaction information including the amount of the purchase and the telephone number (provided by the customer) of mobile unit **12** into cashier register **14** (**FIG. 2**, step **102**). The cashier register generates a transaction ID and transmits transaction information and the mobile unit telephone number

over a land line **16** connected to the PSTN **17** to a financial transaction clearinghouse (clearinghouse) **18** (**FIG. 2,** step **104**). The transaction information includes, for example, a transaction ID, the identity and cost of the goods or services and an identification of the merchant. Clearinghouse **18** receives and records the information (**FIG. 2,** step **106**), then calls mobile unit **12** using the provided telephone number via a cellular system **20** having a base station **22** in the vicinity of the mobile unit **12** (**FIG. 2,** step **108**).

The purchaser answers the incoming telephone call to mobile unit **12** and thereby allows the mobile unit **12** to receive signals transmitted by the clearinghouse **18** (**FIG. 2,** step **110**). Depending upon the implementation, clearinghouse **18** may transmit signals to the mobile unit **12** via the cellular system specifying the amount of the transaction, the identity of the goods or services, and the identity of the merchant. Clearinghouse **18** also transmits a request for either digital money or a financial ID specifying a credit or debit account and approval to charge the account. The mobile unit **12** receives the signals and presents appropriate displays to the customer to display information received from clearinghouse **18** and to request selection of a credit or debit account or digital money (**FIG. 2,** step **112**). To this end, mobile unit **12** retrieves pre-stored financial information from a memory unit (not shown) within the mobile unit identifying the credit and debit accounts of the customer of mobile unit **12** and any digital money stored therein.

An exemplary display is provided in **FIG. 3** within a display screen **24** of mobile unit **12**. As can be seen, the exemplary display identifies the merchant, the goods or services and the amount of the purchase and provides three credit card accounts and two ATM (debit) accounts for selection. The credit card accounts may be, for example, VISA, MASTER CHARGE, and AMERICAN EXPRESS accounts and may be identified by appropriate icons in display screen **24**. (VISA, MASTER CHARGE and AMERICAN EXPRESS are trademarks of their respective companies.) The ATM debit card accounts may be checking accounts maintained at different banks and may be identified by the bank name or other appropriate icons in display screen **24**. The display also shows that the purchase may be made using digital money and specifies the amount of digital money available. Examples involving a digital money purchase will be described below with reference to **FIGS. 11 - 13**.

The customer enters a selection by, for example, pressing the appropriate button on keypad **26** corresponding to the number of the

selected account (**FIG. 2,** step **114**). In the present example the customer selects credit card no. 2 and is presented with the display of **FIG. 4** requesting authorization to bill the amount of the purchase to the selected credit account (**FIG. 2,** step **116**). The customer responds by pressing the appropriate buttons, such as by pressing 1 for YES or 2 for NO. If NO, an appropriate refusal signal is sent to clearinghouse **18** (**FIG. 1**) via cellular system **20** refusing authorization. The refusal is forwarded to the cashier register and the transaction is terminated. Assuming however, that the customer grants approval by selecting YES, the mobile unit retrieves the financial ID for the selected credit account from an internal memory and forwards the financial ID and an authorization signal to the clearinghouse along with transaction ID (**FIG. 2,** step **120**) via cellular system **20**. Although not separately shown, the customer may be required to first enter a personal identification number (PIN) before authorizing the transaction. Also, depending upon the implementation the financial ID may be encrypted, perhaps using a public key encryption system, the details of which are well known to those skilled in the art and will accordingly not be described herein.

Clearinghouse **18** receives the authorization and the selected financial ID from mobile unit **12** along with the transaction ID and contacts the appropriate bank or credit card company to verify that the selected account has sufficient capacity to cover the purchase (**FIG. 2,** step **122**). In **FIG. 1,** an exemplary set of credit card companies **28** and debit card companies **30** are shown. Communications between clearinghouse **18** and the credit and debit card companies may be via PSTN **17** or any other appropriate communications medium. Assuming that the selected account has sufficient capacity for the purchase, the selected credit account company records the amount of the purchase and the transaction ID and sends a verification signal to clearinghouse **18** for forwarding to the cashier register **14** and to mobile unit **12** (**FIG. 2,** step **124**). Hence, both the customer and the merchant are advised simultaneously of the verification (**FIG. 2,** steps **126** and **128**). Both mobile unit **12** and the cashier register **14** provide an appropriate verification display. The telephone call between clearinghouse **18** and the mobile unit **12** is then terminated. The merchant then conveys the goods or services to the customer and the transaction is completed. Ultimately, the credit card company forwards a bill to the customer for the amount of the purchase and forwards funds to the merchant to cover the purchase.

Thus, the system of **FIG. 1** allows for a purchase transaction using, for example, a credit or debit account to be completed easily without requiring the financial ID of the purchasers account to be provided to the merchant and without the use of conventional credit or debit cards which, as noted above, are subject to being lost, stolen or damaged. All of the financial ID's for all of the customers accounts are consolidated in within mobile unit **12** for easy access. Depending upon the implementation, the memory unit of the mobile unit may additionally store the amount of credit or debit remaining, i.e. the account balance, for each credit and debit account. This information may be updated following each transaction. Assuming that all purchases are handled using mobile unit **12**, the account balance information stored therein thereby remains correct. If purchases are made separately perhaps using a conventional credit or debit card, the information for a particular account can be updated following each transaction involving that account by transmitting the current account balance from the appropriate credit or debit card company to the mobile unit via the financial transaction clearinghouse. Additions to the amount of money available in a debit account as a result of a deposit may be tracked in much the same manner.

Depending upon the implementation, the signals transmitted to and from mobile unit **12** may be entirely digital and may be embedded in any on-going voice conversation the purchaser may be having using the mobile unit. For example, for cellular telephone systems employing Code Division Multiple Access (CDMA) technology, which encodes all voice signals digitally, the appropriate digital financial transaction signals may be embedded or interleaved in data packets along with voice signals. In this manner, the purchaser need not terminate an on-going voice telephone call. Rather, the purchaser merely pauses briefly during the conversation to review the information displayed regarding the transaction and to press the appropriate buttons for selecting the credit/debit account and for authorizing the purchase.

Also, depending upon the implementation, no financial transaction clearinghouse is required. Rather, merchant cashier register **14** may communicate directly with the appropriate credit card and debit card companies **28** and **30**.

The messages exchanged during the performance of the steps of the method implemented by the system of **FIG. 1** are summarized at a high level as shown in **FIG. 5** which provides separate time lines **32, 34** and **36** showing, respectively, the steps performed by mobile unit **12**, merchant

cashier register **14** and financial transaction clearinghouse **18** of **FIG. 1**. The steps performed during the generation of the messages shown in **FIG. 5** have already been described with reference to **FIGS. 1** and **2**, and will not be re-described.

With the system and method thus far described, the selected financial ID is transmitted directly from the mobile unit to the financial transaction clearinghouse. Hence the merchant never receives the financial ID. This helps maintain the privacy of the financial ID, particularly from unauthorized use by possible unscrupulous merchants. **FIG. 6** summarizes a somewhat simpler, alternative method wherein the financial ID is transmitted to the merchant cashier register **14**. After the customer indicates a desire to purchase goods or services and provides the telephone number of the mobile unit, the cashier register **14** calls the mobile unit using the telephone number and transmits signals to mobile unit **12** via the cellular system of **FIG. 1**, at step **20**, advising of the transaction and requesting either the financial ID of a credit/debit account or digital money and requesting authorization to complete the transaction. The advise of transaction information includes an identification of the goods or service to be purchased and the cost thereof.

Mobile unit **12** provides appropriate displays such as those illustrated in **FIGS. 3 - 4**, inputs the appropriate selections from the customer and then, assuming that a credit or debit account is selected, transmits the financial ID of the credit or debit account and an authorization signal to the merchant cashier register, step **202**. The cashier register then transmits signals to the financial transaction clearinghouse, step **204**, perhaps using land lines as illustrated in **FIG. 1**, advising of the transaction and providing the financial ID and the authorization signal received from the mobile unit. Again the advice of transaction information includes the cost of the goods or services to be purchased. Clearinghouse **18** forwards the financial ID to the appropriate credit account or debit account company and requests verification that the selected account has the capacity to cover the purchase. Assuming that the selected account has sufficient capacity, a verification signal is received by clearinghouse **18** and then forwarded to the cashier register **14** for completion of the transaction. One particular advantage of performing the method of **FIG. 6** is that the telephone number of the mobile unit need not be provided to the merchant for inputting into the cashier register because no telephone calls are made to the mobile unit.

What has been described thus far is a system wherein communication between the cashier and the financial transaction clearinghouse is

performed using the PSTN and wherein communications between the mobile unit and clearinghouse is performed using a cellular telephone system. In general, however, any appropriate forms of communication may alternatively be employed. For example, communication between the cashier register and the clearinghouse may also be via a cellular telephone system. Alternatively, communications may be performed using a satellite-based mobile communications system. Also, communications between the mobile unit and cashier may be performed using an infrared system.

FIG. 7 illustrates a satellite-based system **310** having a mobile unit **312**, a cashier register **314**, a financial transaction clearinghouse **318**, and credit account and debit account companies **320** and **322** all interconnected via a satellite mobile communications system represented by a single satellite **324**. The satellite system may include ground stations not separately shown. All communications between the various units are performed using the satellite system thereby eliminating the need for any land line communications. Any of the transaction methods described above with respect to **FIGS. 1 - 6** may be performed using the system of **FIG. 7** and the methods will not be re-described.

FIG. 8 illustrates an infrared-based system **410** having a mobile unit **412**, a cashier register **414**, PSTN **417**, a financial transaction clearinghouse **418**, and credit account and debit account companies **428** and **430**. As with the system of **FIG. 1** the cashier register, the clearinghouse and the credit and debit account companies are interconnected via the PSTN. However, communication between the mobile unit and the cashier is performed using infrared signals. More specifically, mobile unit **412** has an infrared receiver/transmitter **424** and cashier register **414** has an infrared receiver/transmitter **426**.

In an exemplary transaction performed in accordance with the method of **FIG. 6**, the cashier transmits to the mobile unit via infrared signals the amount of the transaction and an identification of the goods or services. The mobile unit inputs the customers selection of a credit or debit account, receives explicit authorization from the customer, then transmits the financial ID of the selected account and an authorization signal to the cashier register **414** via infrared signals. Transmission and reception of the infrared signals may be entirely in accordance with conventional infrared techniques which are well understood by those skilled in the art and will not be described herein. In an alternative embodiment of the invention, the method of **FIG. 2** is performed using the system of **FIG. 8** whereby the telephone number of mobile unit **12** is exchanged using the infrared link.

Thus far, in-person transaction methods have been described wherein the customer with mobile unit is in the vicinity of the merchant cashier register. In the following, transactions are described wherein the customer is remote from the merchant and initiates the transaction either via a mobile telephone call to the merchant or via an Internet or similar computer network connection. Also, transactions are described wherein digital money is conveyed.

FIG. 9 illustrates a system **510** having a customer mobile unit **512** and a merchant cashier register **514** with telephone **515**. The mobile unit is located remote from the cashier and telephone as indicated by a dashed line interposed between them. Cashier register **514** and telephone **515** are connected via a land line **516** to PSTN **517** which, in turn, is connected to a financial transaction clearinghouse **518**, cellular system **520** having base station **522**, and credit and debit account companies **528** and **530**. The customer initiates a purchase transaction by calling the merchant telephone **515** using mobile unit **512** and indicates a desire to purchase goods or services. The merchant enters the selected transaction into cashier register **514** which communicates directly with mobile unit **512** via the open mobile telephone call connection to digitally provide the amount and nature of the transaction to the mobile unit and to digitally requests a financial ID and an authorization signal for completing the transaction. This assumes that a mobile system is employed that allows embedding of digital signals within voice telephone conversation signals such as the aforementioned CDMA system. The customer pauses briefly during his conversation with the merchant to select a credit or debit account and to authorize the transaction in the same manner as described above with reference to **FIGS. 3 - 4**. Mobile unit **512** retrieves the financial ID of the selected account and transmits the financial ID and an authorization signal digitally to cashier register **514** again via the same mobile telephone call. Cashier register **514** immediately forwards the financial ID and authorization signal to the financial transaction clearinghouse over a second PSTN line (not separately shown). Clearinghouse **518** operates in the same manner as described above to obtain verification that the selected account has sufficient capacity of the purchase. A verification signal is forwarded back to the cashier **514** which displays the verification to the merchant who verbally conveys the verification to the customer using telephone **515**. Verification may additionally be transmitted from the cashier register to the mobile unit via the open mobile telephone call. The telephone call is then terminated and the transaction is thereafter completed by providing the goods or services to the customer.

The steps of the method implemented by the system of **FIG. 9** are summarized at a high level within **FIG. 10** which provides separate time lines **532**, **534** and **536** showing, respectively, the steps performed by the mobile unit **512**, the cashier register **514** and the financial transaction clearinghouse **518** of **FIG. 9**.

Hence, a system is provided wherein digital signals pertaining to a purchase transaction are transmitted between a customer mobile unit and a merchant cashier register during a voice mobile telephone conversation between the customer and merchant. This is similar to otherwise conventional telephone purchase transactions using credit or debit accounts, but with the system of **FIG. 9 - 10** the customer need not verbally convey the financial ID of a credit/debit account to the merchant during the telephone call. This has the advantage of speeding up the transaction because the customer need not read aloud the financial ID, name and expiration date from a credit card and the merchant need not record that information. Also, mistakes that can commonly occur in reading and transcribing the digits of the financial ID are avoided. Moreover, the unauthorized capture of the financial ID by eavesdropping is minimized. As with previous embodiments, the financial ID may encrypted to further reduce the risk of unauthorized access.

Thus far, all example transactions described have involved the purchase of goods or services using a credit or debit account selected by the customer. As noted above, however, any of the various transaction methods and systems also allow payment for the goods or services using digital money stored within the mobile unit.

FIG. 11 summarizes a digital money transaction using the system of **FIG. 9**. **FIG. 11** provides separate time lines **632** and **634** showing, respectively, the steps performed by the mobile unit **512** and the point of sale cashier register **514** of **FIG. 9**. No time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required. Rather digital money is conveyed for the customer mobile unit to the merchant cashier register.

The customer initiates a purchase transaction with the merchant during a voice mobile telephone call from the mobile unit to the merchant telephone, step **636**. The merchant enters the purchase transaction information into the cashier register and, in the same manner as described above without reference to **FIG. 9**, the cashier register transmits digital signals to the mobile unit advising of the transaction and requesting a financial ID and an authorization signal, step **638**. The customer is then

presented with a display such as is shown in **FIG 3**. However, rather than selecting a credit or debit account, the customer presses the appropriate buttons to select the digital money option and to authorize the purchase. Assuming the customer has sufficient digital money stored within the mobile telephone to cover the purchase, the financial ID or ID's of the digital money is transmitted to the cashier register as digital signals embedded within the mobile telephone voice conversation signals, step **640**. The cashier register receives and stores the digital money. Hence, the digital money account of the mobile unit is decreased and the digital money account of the cashier register is increased. The completion of the digital money transaction is confirmed by transmitting appropriate verification and receipt signals from the cashier register back to the mobile unit, step **642**. The telephone call is then ended and the goods or services are ultimately conveyed to the customer. If the goods or services are for some reason not conveyed, the verification and receipt signals received by the mobile unit of the customer provide proof of the transaction.

Thus far all transactions have been described with reference to systems employing mobile telephones capable of voice conversation telephone calls. As noted above however, purchase transactions can be performed in accordance with the invention using other types of mobile communications units such as laptop computers and PDA's configured with mobile transmitter/receivers. **FIG. 12** provides an example of a system employing a laptop computer wherein a purchase transaction is performed over the Internet. **FIG. 13** illustrates a method using the system of **FIG. 12** wherein the purchase is made with digital money.

FIG. 12 illustrates a system **710** having a mobile laptop computer unit **712** and a merchant computer **714** located remote from one another. Merchant computer **714** is connected via a land line **716** to a PSTN **717** which is in turn connected to a financial transaction clearinghouse **718**, the Internet **719** and a cellular system **720** having a base station **722**. The clearinghouse is additionally connected to various credit account and debit account companies **728** and **730**.

The customer initiates a purchase transaction by contacting the merchant computer via the cellular system and the Internet. In this regard, the laptop computer employs a modem (not separately shown) in connection with a mobile receiver/transmitter (also not separately shown) to contact the merchant computer via base station **722**, cellular system **720**, Internet **719** and PSTN **717** perhaps to access World Wide Web page maintained by the merchant. In any case, the customer selects goods or

services to be purchased by entering the appropriate commands into laptop **712** for transmission to merchant computer **714**.

The merchant computer receives the customers purchase selection and transmits appropriate signals confirming the purchase selection and requesting a financial ID and an authorization signal. As with the other embodiments described above, the customer may select a credit or debit account or a quantity of digital money. If the former, the financial ID of the account is transmitted via the Internet, preferably encrypted, to the merchant computer for forwarding to the financial transaction clearinghouse, perhaps also via the Internet, for verification of adequate credit or debit account capacity. Appropriate, verification signals are sent to the merchant computer and forwarded to the customers laptop computer. If the purchase is via digital money, the financial ID defining the needed quantity of digital money is transmitted over the Internet to the merchant computer, again preferably encoded in some manner to prevent unauthorized capture, and appropriate verification and receipt signals are sent back to the customer. With the digital money transaction, no signal need be sent to the clearinghouse.

FIG. 13 summarizes the digital money transaction using the system of **FIG. 12**. **FIG. 13** provides separate time lines **732** and **734** showing, respectively, the steps performed by the laptop **712** and merchant computer **714** of **FIG. 12**. Again, no time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required.

Various exemplary systems and methods for performing financial transactions such as purchase transactions using a mobile telephone or other mobile communications unit configured to store the financial ID's of various credit and debit accounts and/or quantities of digital money have been described. In accordance with the principles of the invention, a wide variety of other financial transactions may be performed as well including, in general, almost any transaction otherwise handled with credit or debit cards or digital money. Although the examples provided wherein relate to mobile telephone or laptops computers, principles of the invention can be applied to almost any type of mobile communications unit including, the aforementioned PDA's, mobile Internet access devices, etc.

The exemplary embodiments have been primarily described with reference to block diagrams illustrating apparatus elements and timing diagrams and flow charts primarily illustrating method steps. As to the timing diagrams and flowcharts, each block or step therein represents both a

method step and an apparatus element for performing the recited step. Depending upon the implementation, each apparatus element, or portions thereof, may be configured in hardware, software, firmware or combinations thereof. It should be appreciated that not all components necessary for a complete implementation of a practical system are illustrated or described in detail. Rather, only those components necessary for a thorough understanding of the invention have been illustrated and described.

Moreover, the previous description of the preferred embodiments is provided to enable any person skilled in the art to make or use the present invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of the inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WE CLAIM:

CLAIMS

1. In a mobile communications unit, a system for performing a financial transaction comprising:

means for storing a financial identification code; and

means for transmitting said financial identification code to effectuate a financial transaction.

2. The system of claim 1 further including

means for receiving a signal representative of a requested financial transaction; and

means for retrieving the stored financial identification code in response to reception of the signal representative of the requested financial transaction.

3. The system of claim 1 wherein said mobile communications unit is selected from a group consisting of a mobile telephone, a personal data assistant with mobile telephony capability, a laptop computer with mobile telephony capability, an Internet access device with mobile telephony capability, and an electronic organizer with mobile telephony capability.

4. The system of claim 1 wherein said financial identification code is representative of digital money.

5. The system of claim 1 wherein said financial identification code is representative of a debit account.

6. The system of claim 1 wherein said financial identification code is representative of a credit account.

7. The system of claim 1 wherein said means for storing a financial identification code stores a plurality of financial identification codes.

8. The system of claim 7 wherein said system further includes -

means for providing an indication representative of said financial identification codes and for requesting selection of one to effectuate transaction; and

means for receiving a selection signal representative of one of said financial identification codes.

9. The system of claim 2 further comprising:

means for providing an indication of said requested financial transaction and for requesting approval to effectuate transaction;

means for receiving an authorization signal representative of whether approval is granted for effectuating said requested transaction; and

means for transmitting said authorization signal.

10. The system of claim 9 wherein said means for receiving an authorization signal operates to receive a personal identification number code.

11. The system of claim 4 further including

means for receiving a signal indicative of a completed financial transaction; and

means for modifying said digital money financial identification code to reflect the completed financial transaction.

12. The system of claim 2

wherein said means for receiving the signal representative of the requested financial transaction includes an infrared receiver.

13. The system of claim 1

wherein said means for transmitting said financial identification code includes an infrared transmitter.

14. The system of claim 2

wherein said means for receiving the signal representative of the requested financial transaction includes a cellular telephone receiver.

15. The system of claim 1

wherein said means for transmitting said financial identification code includes a cellular telephone transmitter.

16. The system of claim 2 wherein said means for receiving the signal representative of the requested financial transaction includes a wireless telephone receiver for receiving signals from a satellite.

17. The system of claim 1 wherein said means for transmitting said financial identification code includes a wireless telephone transmitter for transmitting signals to a satellite.

18. The system of claim 1 wherein said means for transmitting said financial identification code includes a means for encrypting the financial identification code prior to transmission.

19. In a mobile communications unit, a system for performing a financial transaction comprising:

a memory unit storing a financial identification code;

a receive unit receiving a signal representative of a requested financial transaction;

a control unit retrieving the financial identification code in response the received signal; and

a transmit unit transmitting said financial identification code to effectuate said requested financial transaction.

20. A system for performing a financial transaction comprising:

a point of sale unit comprising

means for transmitting a signal representative of a requested financial transaction, and

means for receiving a financial identification code for effectuating said requested financial transaction;

a mobile communications unit comprising

means for storing a financial identification code,

means for receiving the signal representative of the requested financial transaction, and

means for transmitting said financial identification code to effectuate said requested financial transaction.

21. In a mobile communications unit, a method for performing a financial transaction comprising the steps of:

storing a financial identification code; and

transmitting said financial identification code to effectuate a financial transaction.

22. The method of claim 21 further including the steps of

receiving a signal representative of a requested financial transaction; and

retrieving the stored financial identification code for transmission in response to reception of the signal representative of a requested financial transaction.

23. The method of claim 21 wherein said mobile communications unit is selected from a group consisting of a mobile telephone, a personal data assistant with mobile telephony capability, a laptop computer with mobile telephony capability, an Internet access device with mobile telephony capability, and an electronic organizer with mobile telephony capability.

24. The method of claim 21 wherein said financial identification code is representative of digital money.

25. The method of claim 21 wherein said financial identification code is representative of a debit account.

26. The method of claim 21 wherein said financial identification code is representative of a credit account.

27. The method of claim 21 wherein said step of storing a financial identification code is performed to store a plurality of financial identification codes.

28. The method of claim 27 wherein said method further includes the steps of

providing an indication representative of said financial identification codes and for requesting selection of one to effectuate said transaction; and

receiving a selection signal representative of one of said financial identification codes.

29. The method of claim 23 further comprising the steps of:

providing an indication of said requested financial transaction and for requesting approval to effectuate said transaction;

receiving an authorization signal representative of whether approval is granted for effectuating said transaction; and

transmitting said authorization signal.

30. The method of claim 21 wherein said step of receiving a authorization signal is performed to receive a personal identification number code.

31. The method of claim 24 further including the steps of

receiving a signal indicative of a completed financial transaction; and

modifying said digital money financial identification code to reflect the completed financial transaction.

32. The method of claim 22

wherein said step of receiving the signal representative of the requested financial transaction includes the step of receiving an infrared signal.

33. The method of claim 21

wherein said step of transmitting said financial identification code includes the step of transmitting an infrared signal.

34. The method of claim 22

wherein said step of receiving the signal representative of the requested financial transaction includes the step of receiving a cellular telephone signal.

35. The method of claim 21

wherein said step of transmitting said financial identification code includes the step of transmitting a cellular telephone signal.

36. The method of claim 22

wherein said step of receiving the signal representative of the requested financial transaction includes the step receiving signals from a satellite.

37. The method of claim 21

2 wherein said step of transmitting said financial identification code includes the step of transmitting signals to a satellite.

38. The method of claim 21 wherein said step of transmitting said

2 financial identification code includes the step of encrypting the financial identification code prior to transmission.

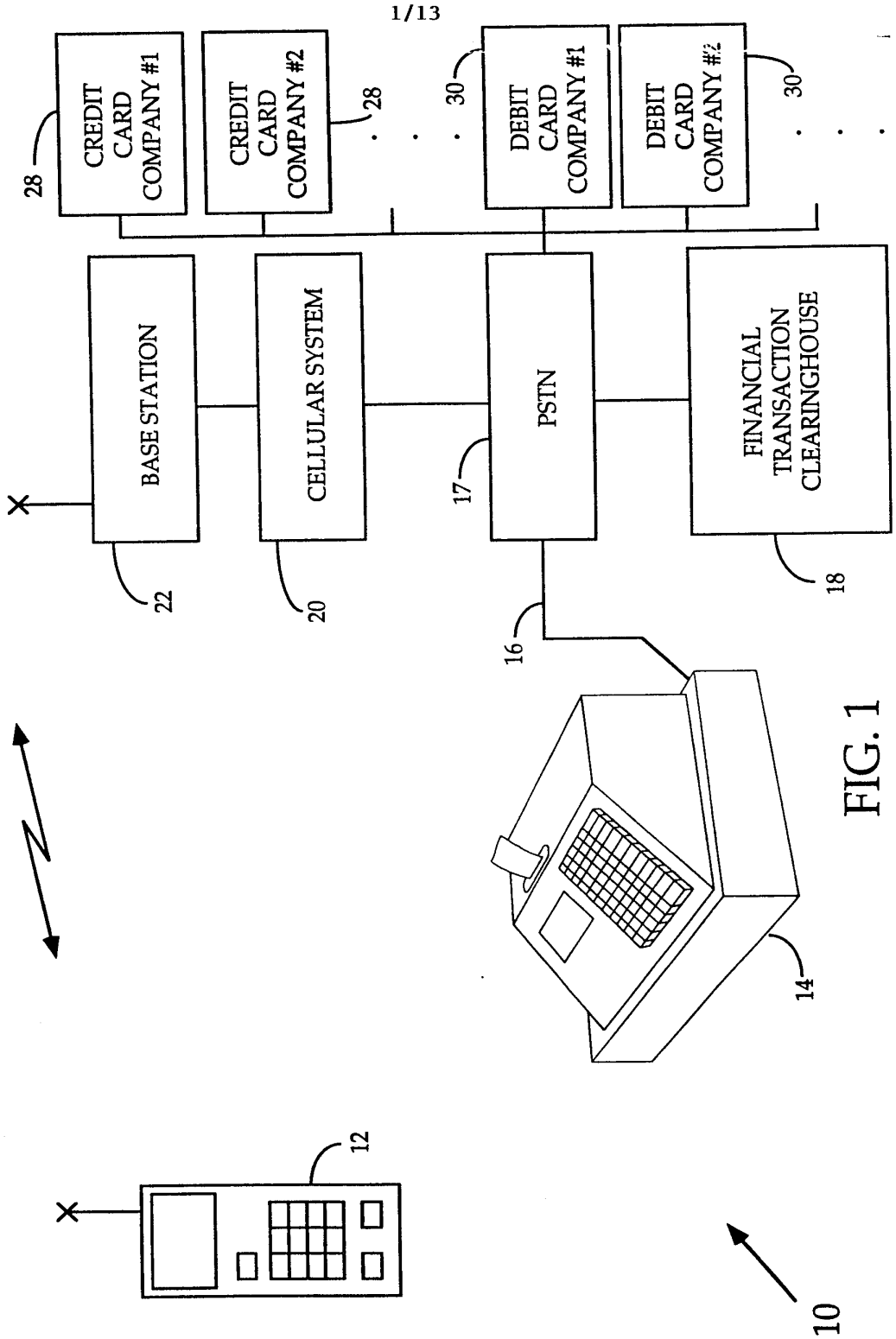

CREDIT CARD COMPANY #1
CREDIT CARD COMPANY #2
DEBIT CARD COMPANY #1
DEBIT CARD COMPANY #2
28
30
BASE STATION
CELLULAR SYSTEM
PSTN
FINANCIAL TRANSACTION CLEARINGHOUSE
17
22
20
18
16
14
12
10

FIG. 1

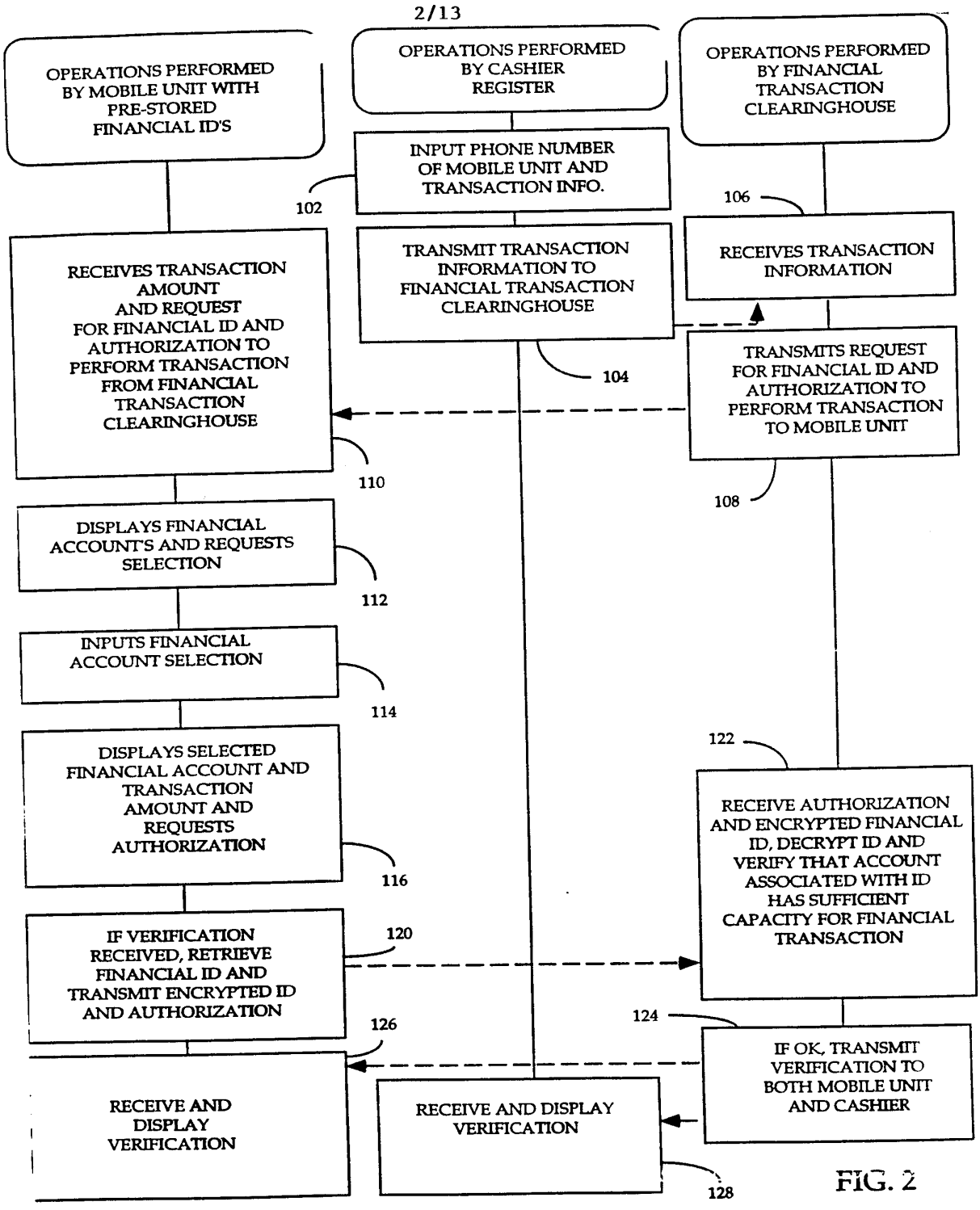

OPERATIONS PERFORMED BY MOBILE UNIT WITH PRE-STORED FINANCIAL ID'S
OPERATIONS PERFORMED BY CASHIER REGISTER
OPERATIONS PERFORMED BY FINANCIAL TRANSACTION CLEARINGHOUSE
INPUT PHONE NUMBER OF MOBILE UNIT AND TRANSACTION INFO.
102
106
RECEIVES TRANSACTION AMOUNT AND REQUEST FOR FINANCIAL ID AND AUTHORIZATION TO PERFORM TRANSACTION FROM FINANCIAL TRANSACTION CLEARINGHOUSE
TRANSMIT TRANSACTION INFORMATION TO FINANCIAL TRANSACTION CLEARINGHOUSE
RECEIVES TRANSACTION INFORMATION
104
TRANSMITS REQUEST FOR FINANCIAL ID AND AUTHORIZATION TO PERFORM TRANSACTION TO MOBILE UNIT
110
108
DISPLAYS FINANCIAL ACCOUNT'S AND REQUESTS SELECTION
112
INPUTS FINANCIAL ACCOUNT SELECTION
114
122
DISPLAYS SELECTED FINANCIAL ACCOUNT AND TRANSACTION AMOUNT AND REQUESTS AUTHORIZATION
116
RECEIVE AUTHORIZATION AND ENCRYPTED FINANCIAL ID, DECRYPT ID AND VERIFY THAT ACCOUNT ASSOCIATED WITH ID HAS SUFFICIENT CAPACITY FOR FINANCIAL TRANSACTION
IF VERIFICATION RECEIVED, RETRIEVE FINANCIAL ID AND TRANSMIT ENCRYPTED ID AND AUTHORIZATION
120
124
126
IF OK, TRANSMIT VERIFICATION TO BOTH MOBILE UNIT AND CASHIER
RECEIVE AND DISPLAY VERIFICATION
RECEIVE AND DISPLAY VERIFICATION
128

FIG. 2

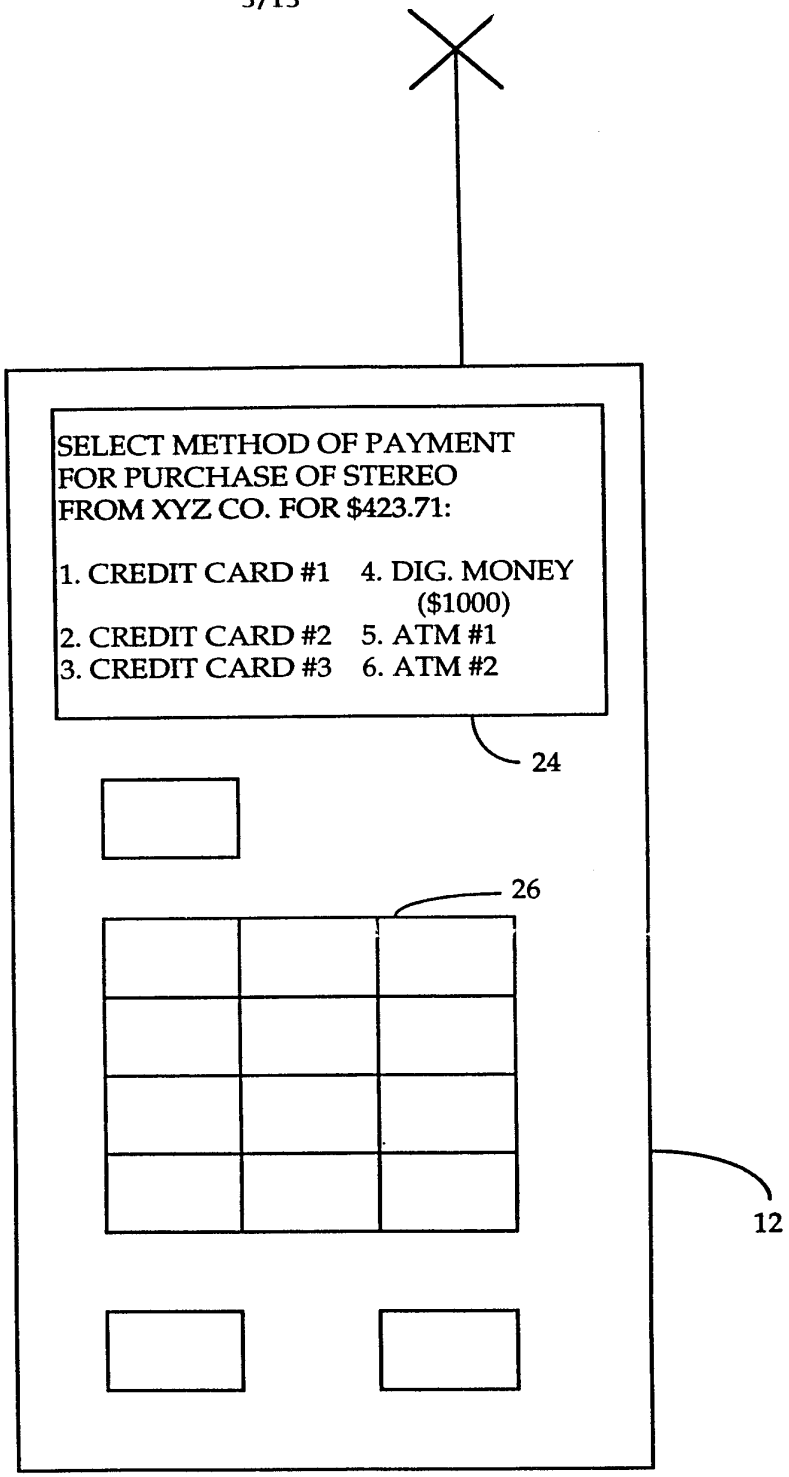

SELECT METHOD OF PAYMENT
FOR PURCHASE OF STEREO
FROM XYZ CO. FOR $423.71:
1. CREDIT CARD #1
2. CREDIT CARD #2
3. CREDIT CARD #3
4. DIG. MONEY ($1000)
5. ATM #1
6. ATM #2
24
26
12

FIG. 3

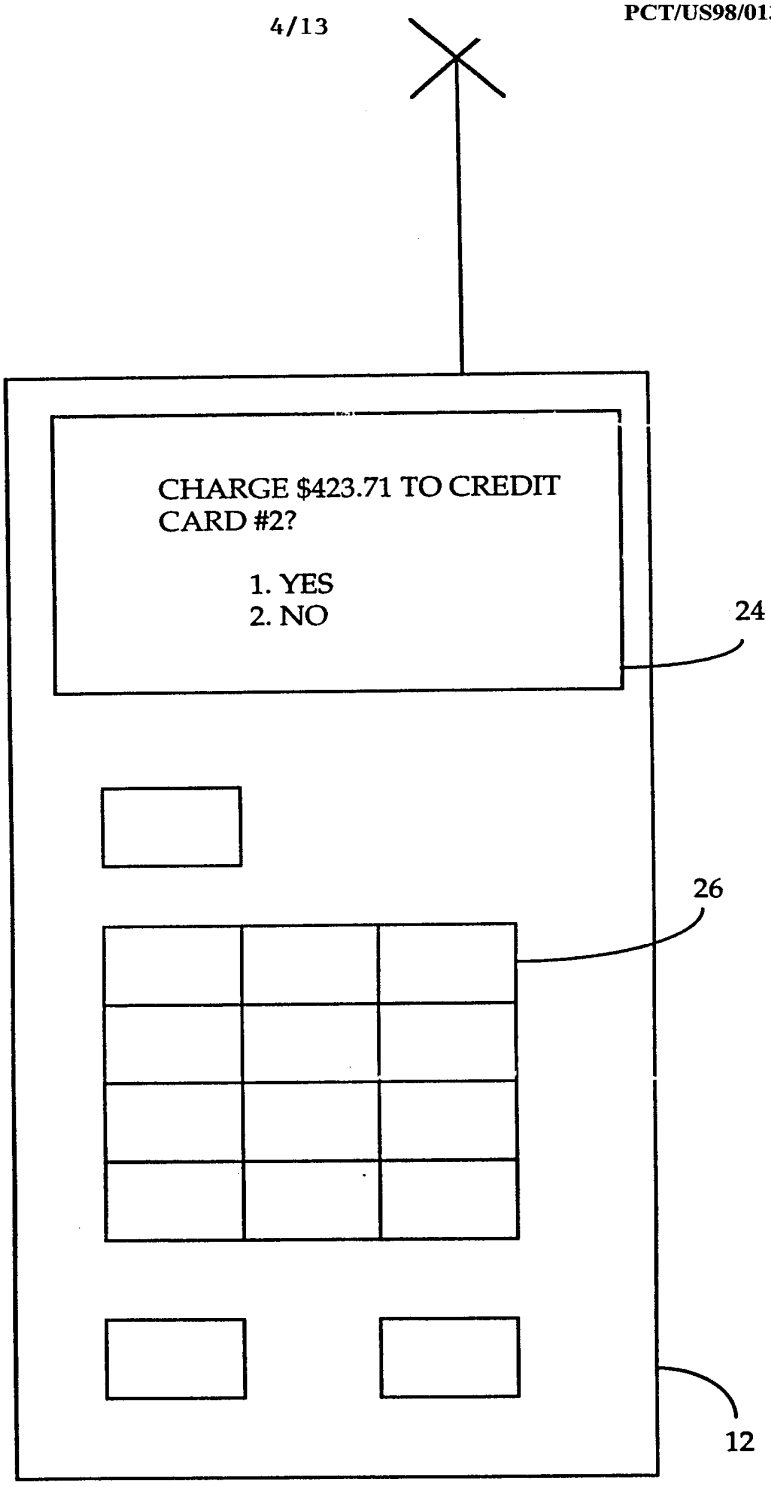


FIG. 4

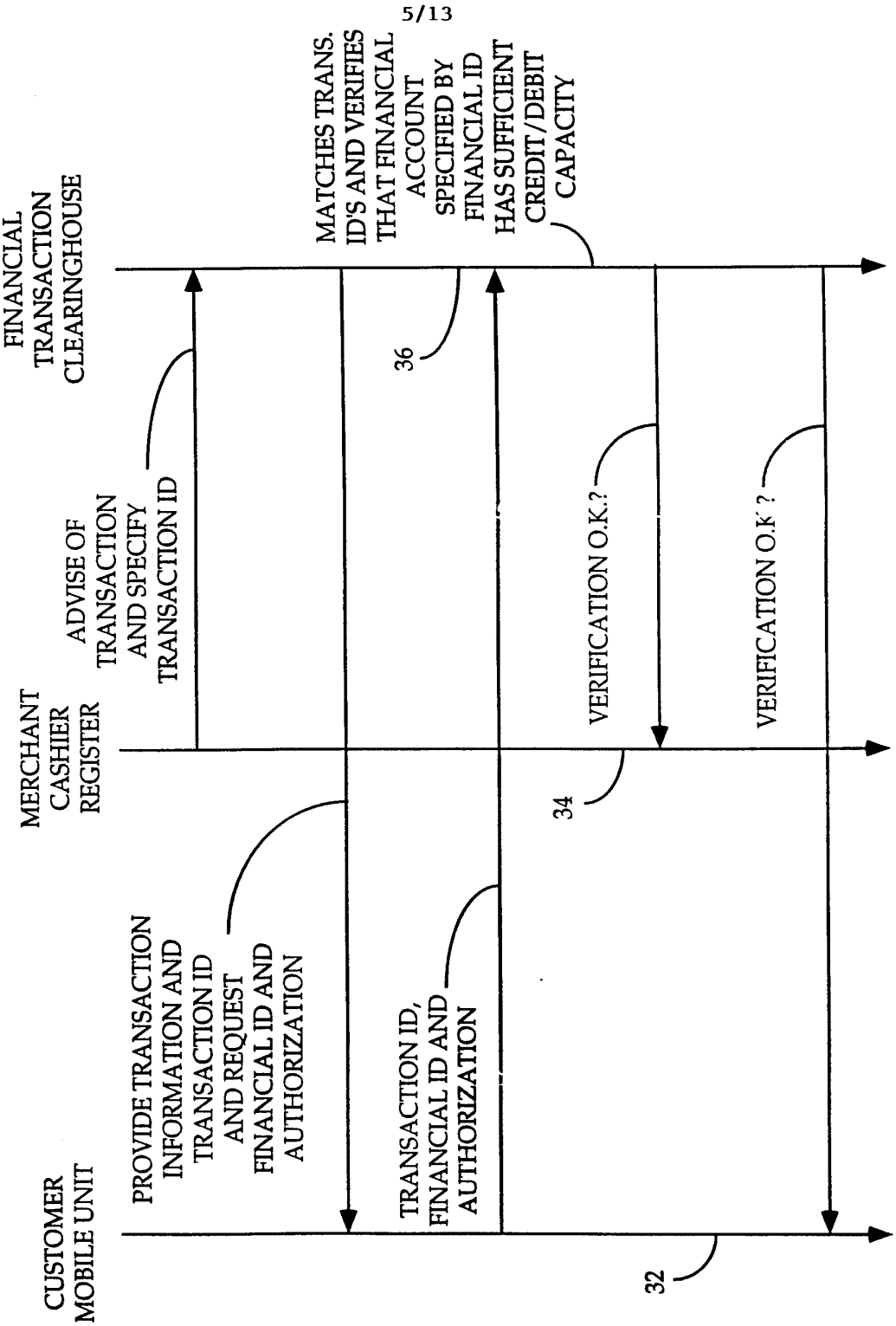

FINANCIAL TRANSACTION CLEARINGHOUSE
MERCHANT CASHIER REGISTER
CUSTOMER MOBILE UNIT
ADVISE OF TRANSACTION AND SPECIFY TRANSACTION ID
PROVIDE TRANSACTION INFORMATION AND TRANSACTION ID AND REQUEST FINANCIAL ID AND AUTHORIZATION
TRANSACTION ID, FINANCIAL ID AND AUTHORIZATION
MATCHES TRANS. ID'S AND VERIFIES THAT FINANCIAL ACCOUNT SPECIFIED BY FINANCIAL ID HAS SUFFICIENT CREDIT/DEBIT CAPACITY
VERIFICATION O.K.?
VERIFICATION O.K.?
36
34
32

FIG. 5

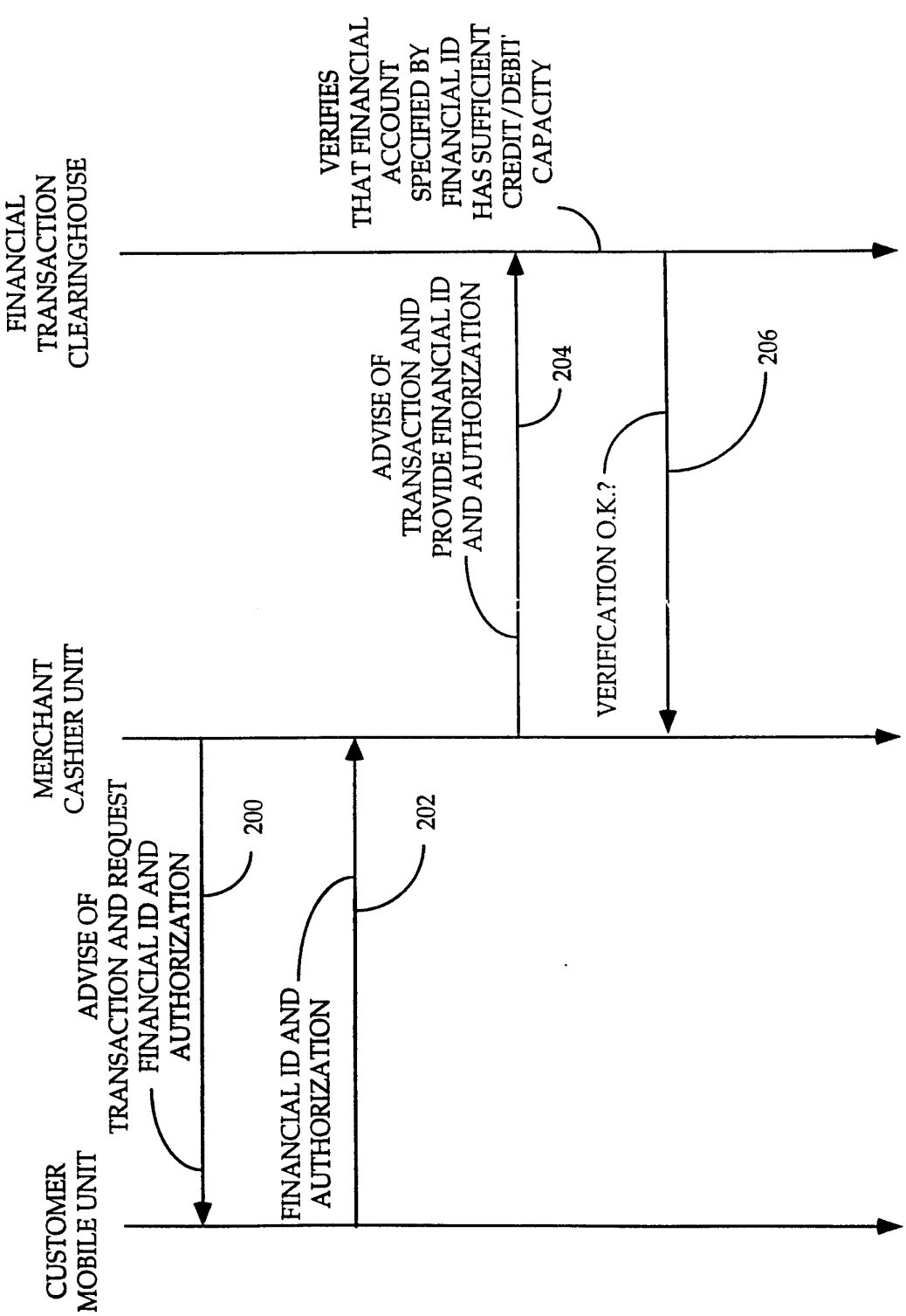

CUSTOMER MOBILE UNIT
MERCHANT CASHIER UNIT
FINANCIAL TRANSACTION CLEARINGHOUSE
ADVISE OF TRANSACTION AND REQUEST FINANCIAL ID AND AUTHORIZATION
200
FINANCIAL ID AND AUTHORIZATION
202
ADVISE OF TRANSACTION AND PROVIDE FINANCIAL ID AND AUTHORIZATION
204
VERIFIES THAT FINANCIAL ACCOUNT SPECIFIED BY FINANCIAL ID HAS SUFFICIENT CREDIT/DEBIT CAPACITY
VERIFICATION O.K.?
206

FIG. 6

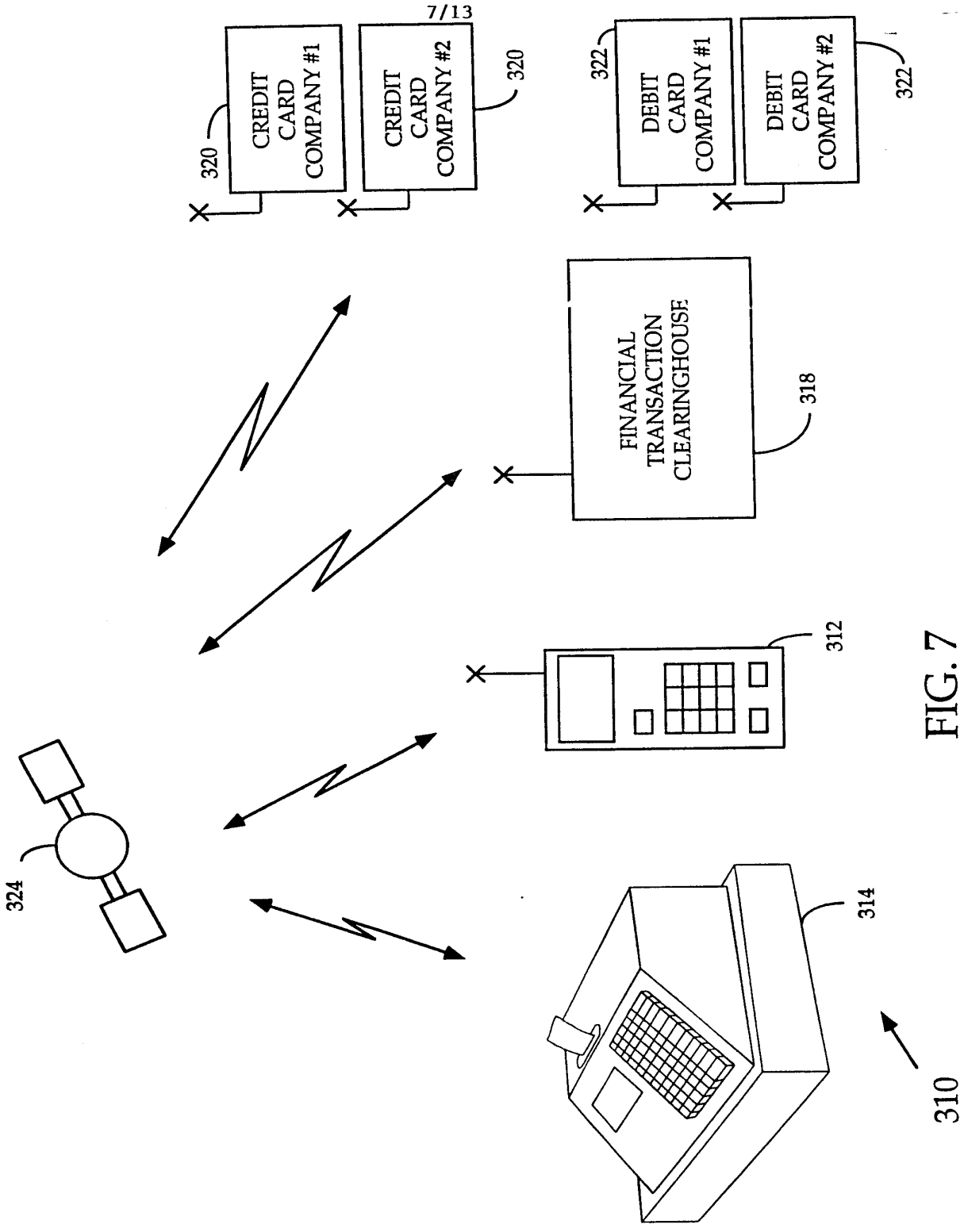

CREDIT CARD COMPANY #1
320
CREDIT CARD COMPANY #2
320
DEBIT CARD COMPANY #1
322
DEBIT CARD COMPANY #2
322
FINANCIAL TRANSACTION CLEARINGHOUSE
318
312
324
314
310

FIG. 7

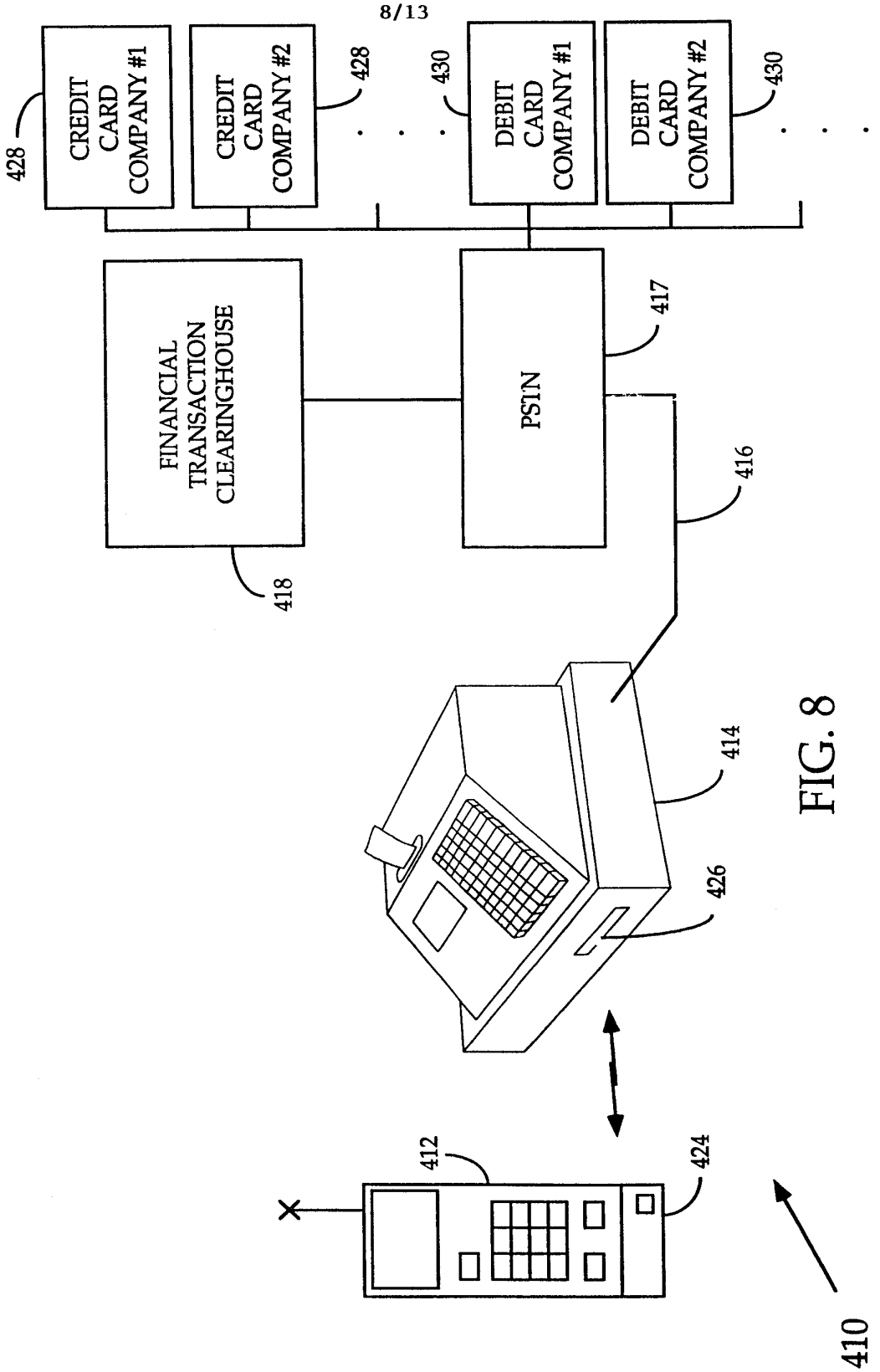

CREDIT CARD COMPANY #1
CREDIT CARD COMPANY #2
DEBIT CARD COMPANY #1
DEBIT CARD COMPANY #2
428
428
430
430
FINANCIAL TRANSACTION CLEARINGHOUSE
418
PSTN
417
416
414
426
412
424
410

FIG. 8

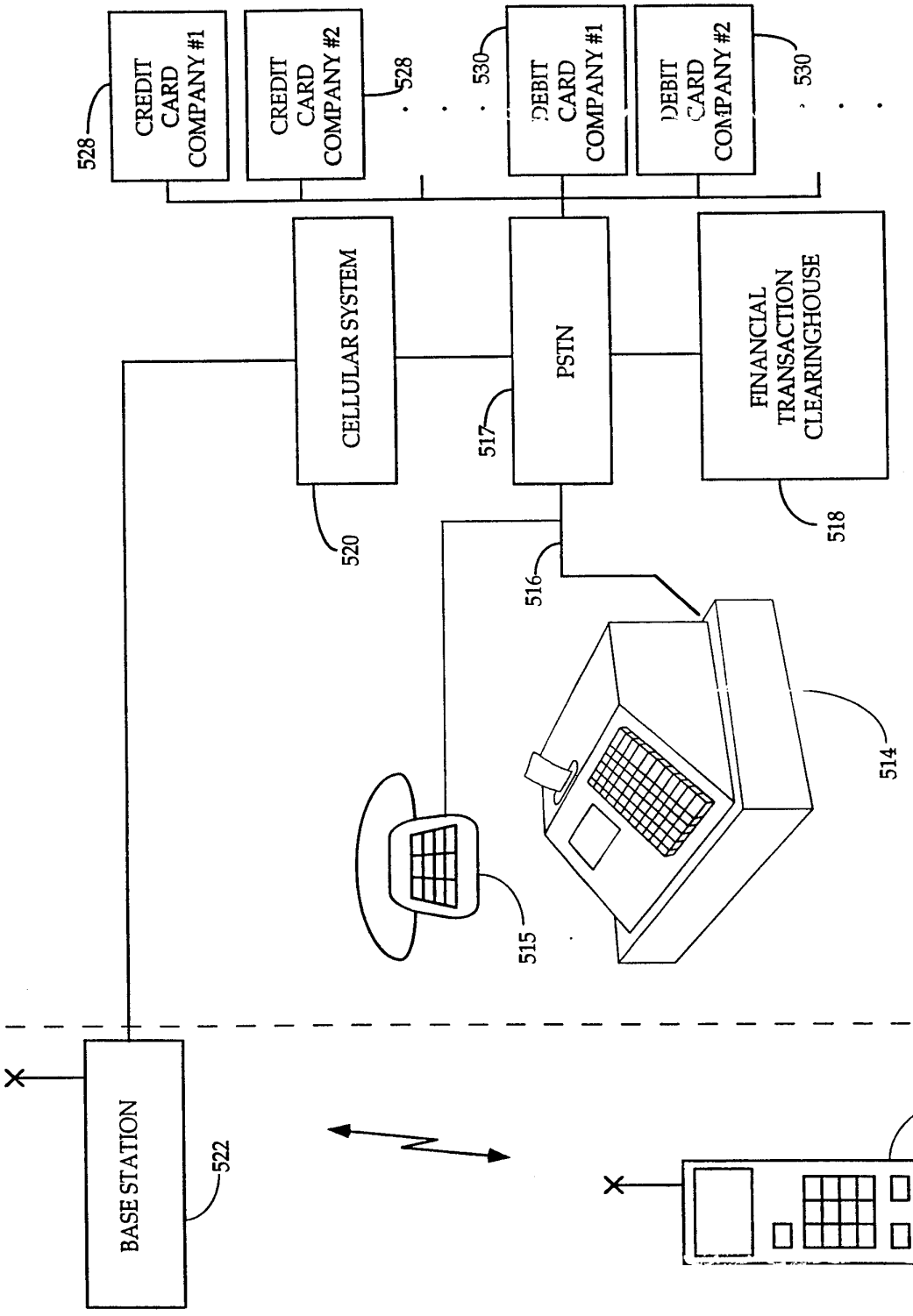

CREDIT CARD COMPANY #1
CREDIT CARD COMPANY #2
DEBIT CARD COMPANY #1
DEBIT CARD COMPANY #2
528
528
530
530
CELLULAR SYSTEM
PSTN
FINANCIAL TRANSACTION CLEARINGHOUSE
517
520
516
518
514
515
510
BASE STATION
522
512

FIG. 9

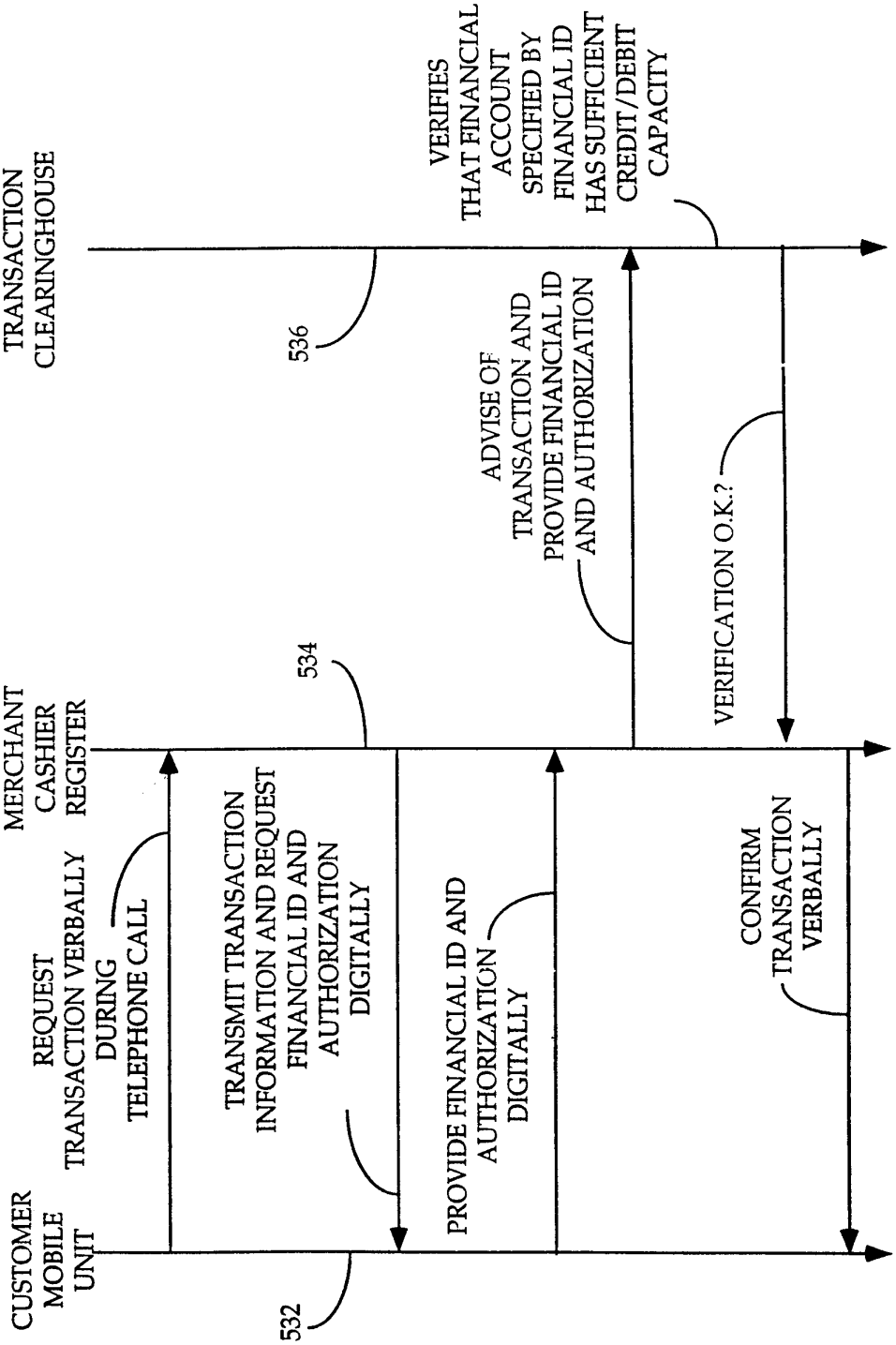

CUSTOMER MOBILE UNIT
MERCHANT CASHIER REGISTER
FINANCIAL TRANSACTION CLEARINGHOUSE
REQUEST TRANSACTION VERBALLY DURING TELEPHONE CALL
TRANSMIT TRANSACTION INFORMATION AND REQUEST FINANCIAL ID AND AUTHORIZATION DIGITALLY
PROVIDE FINANCIAL ID AND AUTHORIZATION DIGITALLY
CONFIRM TRANSACTION VERBALLY
END TELEPHONE CALL
532
534
536
ADVISE OF TRANSACTION AND PROVIDE FINANCIAL ID AND AUTHORIZATION
VERIFIES THAT FINANCIAL ACCOUNT SPECIFIED BY FINANCIAL ID HAS SUFFICIENT CREDIT/DEBIT CAPACITY
VERIFICATION O.K.?

FIG. 10

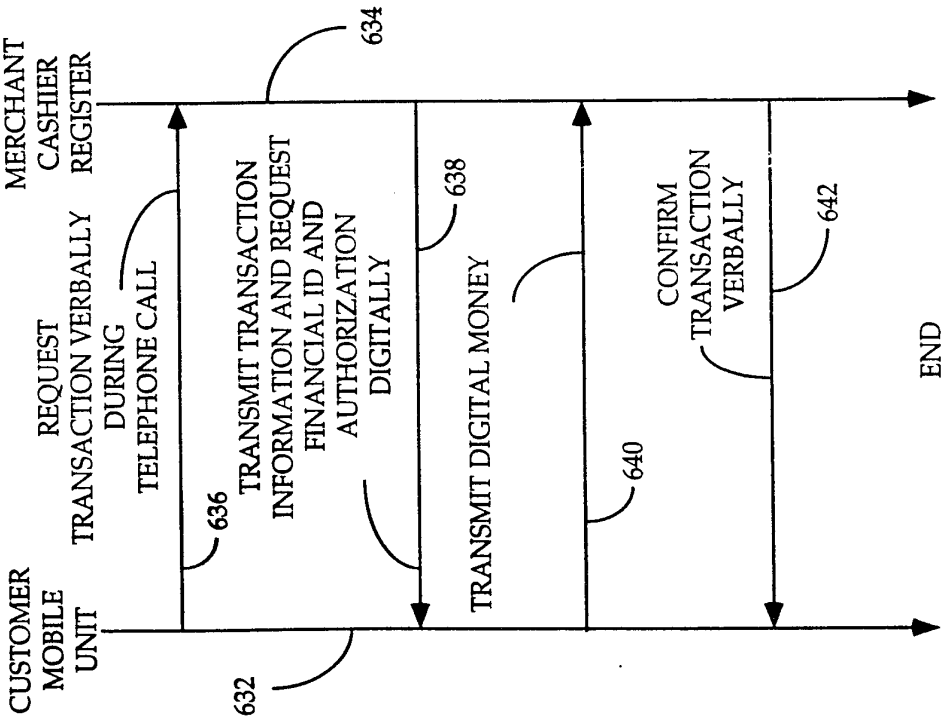

CUSTOMER MOBILE UNIT
MERCHANT CASHIER REGISTER
632
634
636
638
640
642
REQUEST TRANSACTION VERBALLY DURING TELEPHONE CALL
TRANSMIT TRANSACTION INFORMATION AND REQUEST FINANCIAL ID AND AUTHORIZATION DIGITALLY
TRANSMIT DIGITAL MONEY
CONFIRM TRANSACTION VERBALLY
END TELEPHONE CALL

FIG. 11

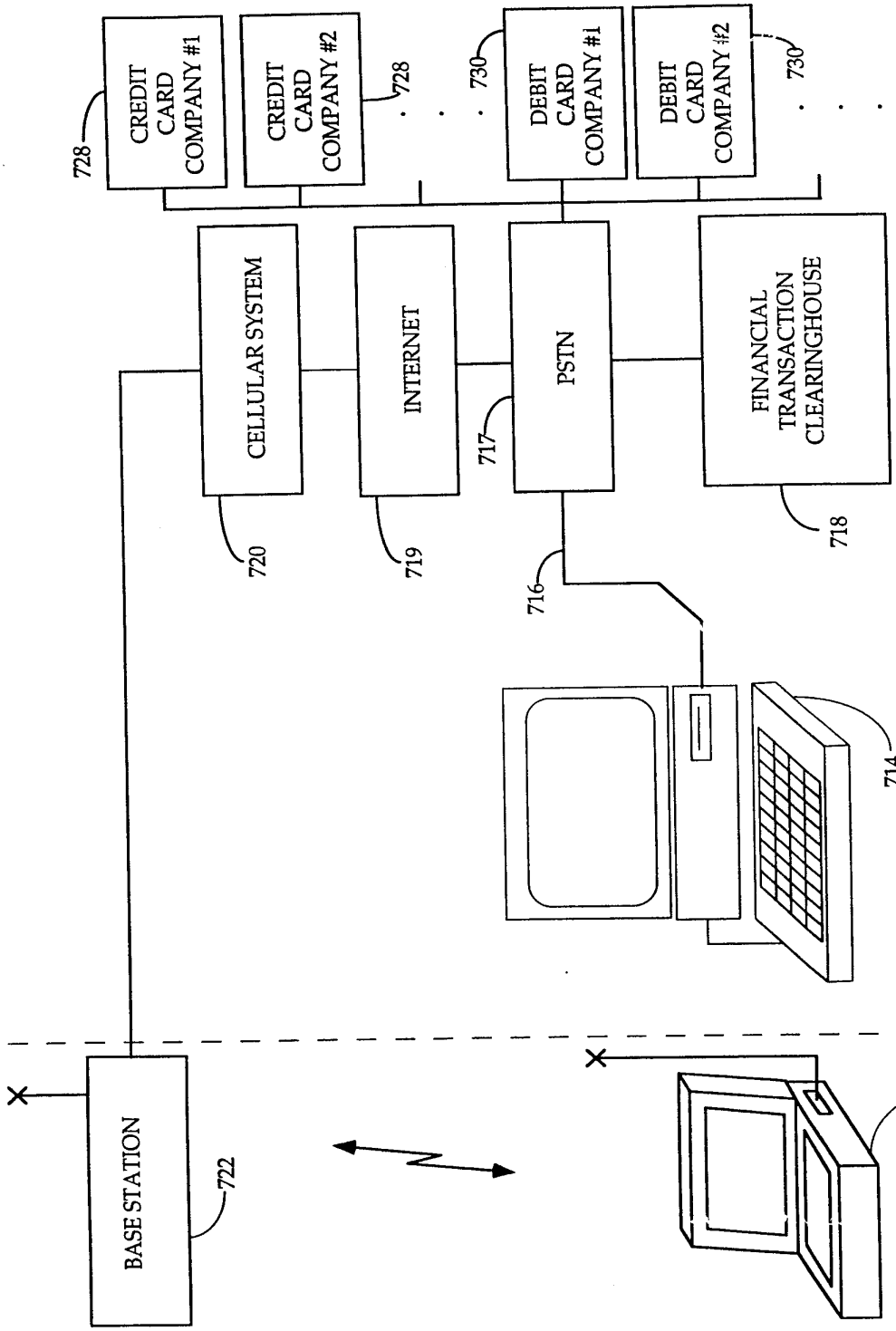

CREDIT CARD COMPANY #1
CREDIT CARD COMPANY #2
DEBIT CARD COMPANY #1
DEBIT CARD COMPANY #2
728
730
CELLULAR SYSTEM
INTERNET
PSTN
FINANCIAL TRANSACTION CLEARINGHOUSE
717
720
719
718
716
714
712
BASE STATION
722
710

FIG. 12

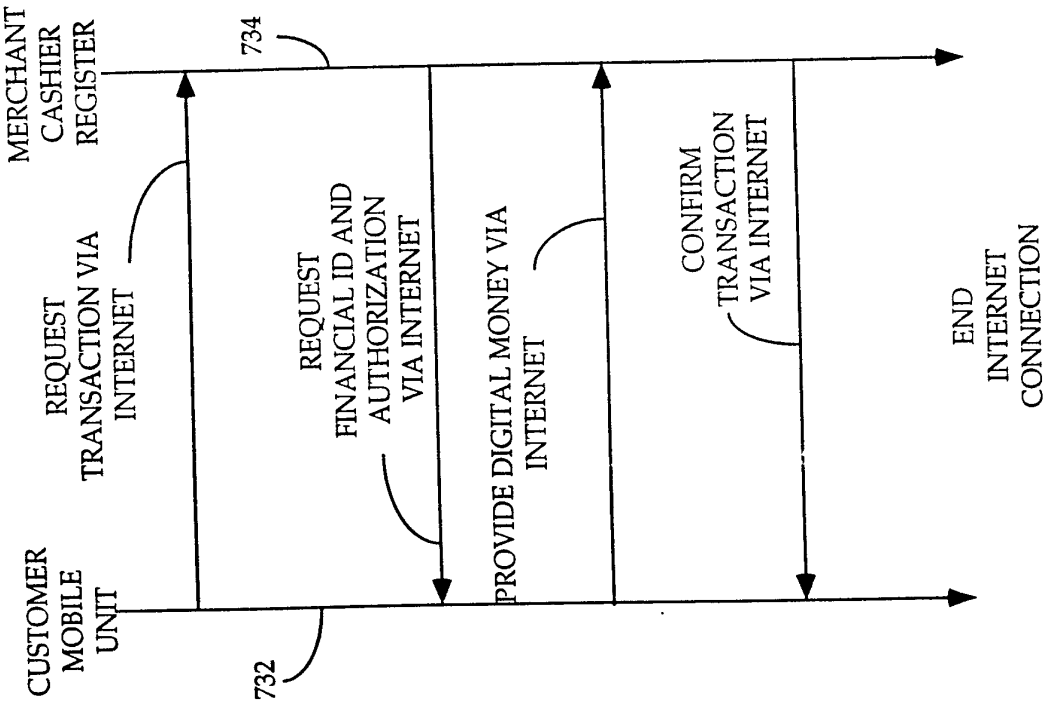

MERCHANT CASHIER REGISTER
734
REQUEST TRANSACTION VIA INTERNET
REQUEST FINANCIAL ID AND AUTHORIZATION VIA INTERNET
PROVIDE DIGITAL MONEY VIA INTERNET
CONFIRM TRANSACTION VIA INTERNET
END INTERNET CONNECTION
CUSTOMER MOBILE UNIT
732

FIG. 13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 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 6 G07F H04M

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 96 25828 A (NOKIA MOBILE PHONES) 22 August 1996 see abstract; claims; figures 1,6,7 see page 13, line 3 - page 19, line 28	1,3-7, 21,23-27 8,10-15, 19,20, 28,30-35
A	WO 94 11849 A (H.T. VATANEN) 26 May 1994 see abstract; claims; figures see page 5, line 36 - page 11, line 10	1,3,5,6, 9,10, 12-15, 19-21, 23,25, 26,29, 30,32-35
A	EP 0 708 547 A (AT & T) 24 April 1996	

-/--

[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
7 July 1998	15/07/1998

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	David, J

1

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

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

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 96 13814 A (B. VAZVAN) 9 May 1996	

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/01391

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9625828 A	22-08-1996	FI 950685 A	16-08-1996
		AU 4624796 A	04-09-1996
		EP 0809916 A	03-12-1997
WO 9411849 A	26-05-1994	FI 925135 A	12-05-1994
		FI 934995 A	12-05-1994
		AT 159602 T	15-11-1997
		DE 69314804 D	27-11-1997
		EP 0669031 A	30-08-1995
		ES 2107689 T	01-12-1997
		NO 951814 A	09-05-1995
EP 0708547 A	24-04-1996	US 5608778 A	04-03-1997
		CA 2156206 A	23-03-1996
		JP 8096043 A	12-04-1996
WO 9613814 A	09-05-1996	FI 945075 A	29-04-1996
		EP 0739526 A	30-10-1996
		FI 962553 A	25-11-1997
		FI 962961 A	28-08-1996
		FI 971009 A	26-04-1997
		FI 971248 A	26-04-1997
		FI 971848 A	30-04-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年12 月20 日 (20.12.2001)

PCT

(10) 国際公開番号
WO 01/97118 A1

(51) 国際特許分類[7]: G06F 17/60, 19/00

(21) 国際出願番号: PCT/JP01/05039

(22) 国際出願日: 2001 年6 月13 日 (13.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-178188 2000 年6 月14 日 (14.06.2000) JP
特願2000-221240 2000 年7 月21 日 (21.07.2000) JP
特願2000-402918 2000 年12 月28 日 (28.12.2000) JP

(71) 出願人 および
(72) 発明者: 浄弘貴子 (JOGU, Takako) [JP/JP]; 〒631-0036 奈良県奈良市学園北1丁目8番4号 Nara (JP). 與　貞行 (ATAE, Sadayuki) [JP/JP]; 〒815-0071 福岡県福岡市南区平和2-4-10-402 Fukuoka (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, US, UZ, VN, YU, ZA, ZW.

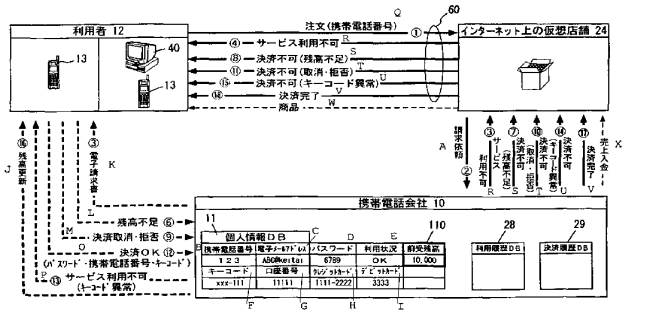
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: SETTLING METHOD USING MOBILE PHONE AND MOBILE PHONE

(54) 発明の名称: 携帯電話機を用いた決済方法および携帯電話機



12...USER
Q...ORDER (MOBILE PHONE NUMBER)
R...SERVICE USE NOT PERMITTED
S...SETTLEMENT NOT PERMITTED (BALANCE IN THE RED)
T...SETTLEMENT NOT PERMITTED (CANCELLED, REJECTED)
U...SETTLEMENT NOT PERMITTED (ABNORMAL KEYCODE)
V...SETTLEMENT COMPLETED
W...COMMODITY
24...VIRTUAL STORE ON INTERNET
A...BILLING REQUEST
X...SALES PAYMENT CREDITED
11...PERSONAL INFORMATION DB
10...MOBILE PHONE FIRM
B...MOBILE PHONE NUMBER
C...E-MAIL ADDRESS
D...PASSWORD
E...USAGE STATUS
110...ADVANCE PAYMENT BALANCE
28...USAGE HISTORY DB
29...SETTLEMENT HISTORY DB
F...KEYCODE
G...ACCOUNT NUMBER
H...CREDIT CARD
I...DEBIT CARD
J...BALANCE UPDATING
K...ELECTRONIC BILLING
L...BALANCE IN THE RED
M...SETTLEMENT CANCELLED/REJECTED
O...SETTLEMENT OK (PASSWORD/MOBILE PHONE NUMBER/KEYCODE)
P...SERVICE USE NOT PERMITTED (ABONORMAL KEYCODE)

(57) Abstract: A virtual account (110) is opened in a mobile phone firm (10) for each user (12) of a mobile phone (13). A user (12) deposits advance payment in a virtual account (110) using a mobile phone (13). Advance payment is paid in combination with telephone charges or by means of a credit card or a debit card. A balance of a virtual account is stored in

[続葉有]

WO 01/97118 A1

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

a mobile phone (13). When shopping at a virtual store on the Internet, the phone number of a mobile phone (13) is transmitted, and , when shopping at a real store, the phone number is sent to a POS terminal. Each store bills a settlement amount to a mobile phone firm. Therefore, settlement can be made with high security and simplicity by using a mobile phone.

(57) 要約:

携帯電話機（１３）の利用者（１２）ごとに携帯電話会社（１０）内に仮想口座（１１０）を設ける。利用者（１２）は携帯電話機（１３）を用いて仮想口座（１１０）に前払金を入金しておく。前払金は、通話料と合せて支払ったり、クレジットカードやデビットカードで支払う。携帯電話機（１３）には仮想口座（１１０）の残高が記憶されている。インターネット上の仮想店舗で買物をする場合は携帯電話機（１３）の電話番号を送信し、実在店舗で買物をする場合は電話番号をＰＯＳ端末に送信する。各店舗は、携帯電話会社（１０）に決済金額を請求する。したがって、高いセキュリティで簡単に携帯電話機を用いて決済することができる。

明細書

携帯電話機を用いた決済方法および携帯電話機

技術分野

この発明は、携帯電話機およびその携帯電話機を用いた決済方法に関し、さらに詳しくは、インターネット上の仮想店舗や実在店舗における決済を仲介するサービスに関する。

背景技術

現在、携帯電話機を用いた種々の決済方法が提案されている。日経エレクトロニクス「携帯で決済」第７６９号, 日経ＢＰ社(２０００年５月８日) 発行, １０９～１２９頁には、ＩＣカードを搭載した携帯電話機が記載されている。この携帯電話機では、ＩＣカードにクレジットカード番号をセキュアな状態で予め記録しておき、決済時にクレジットカード番号を暗号化して送信するようにしている。また、非接触型ＩＣカード用のリーダ／ライタを搭載した携帯電話機も記載されている。この携帯電話機では、プリペイドカードの度数のような電子バリューをダウンロードし、これをリーダ／ライタにより非接触型ＩＣカードに無線経由で転送するようにしている。利用者はこの非接触型ＩＣカードを使って決済を行なう。

上記ＩＣカードを搭載した携帯電話機ではクレジットカード番号を暗号化しているが、クレジットカード番号を送信していることに変わりはないので、インターネット上の電子商取引では十分なセキュリティとは言えない。

一方、上記リーダ／ライタを搭載した携帯電話機では、利用者は携帯電話機とともに非接触型ＩＣカードを持ち歩かなければならない。また、リーダ／ライタはサイズが大きく、コストも高いなど、問題も多い。

この他、携帯電話機を用いた種々の決済方法が提案されているが、いずれも決済時に与信照会が必要であったり、決済データの送信が必要なため、決済時に電波を飛ばす必要があり、電波圏外では使用することができず、また、決済に時間

がかかるという問題がある。

発明の開示

この発明は、上記のような問題を解決するためになされたもので、セキュリティが高く使い勝手のよい携帯電話機およびその携帯電話機を用いた決済方法を提供することを目的とする。

この発明による携帯電話機を用いた決済方法は、売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、利用者の金銭を蓄積するための口座を利用者ごとに設けたサーバコンピュータにおいて、携帯電話機から送信された金額を受信するステップと、受信した金額を利用者の口座に入金してその口座の残高を更新するステップと、更新した口座の残高を携帯電話機に送信するステップと、決済金額を受信するステップと、受信した決済金額を口座の残高から減じるステップと、受信した決済金額を売り主に支払うステップとを含む。ここでのサーバコンピュータは、携帯電話局（会社）、金融機関（会社）、決済機関（会社）などに設置され得るが、その位置は特に限定されない。

一方、この発明による携帯電話機は、売り主と携帯電話機の利用者たる買い主との間の決済に用いられる携帯電話機であって、利用者の金銭を蓄積するための口座がサーバコンピュータに利用者ごとに設けられ、利用者の操作に応じて口座に入金される所望の金額を入力する手段と、入力された金額を携帯電話局のコンピュータに送信し、サーバコンピュータから送信された仮想口座の残高を受信する送受信手段と、受信した口座の残高を記憶する手段とを備える。

この決済方法または携帯電話機によれば、利用者は携帯電話機を用いて所望の金額を携帯電話局または携帯電話局を通じて金融機関もしくは決済機関に送信する。携帯電話局、金融機関または決済機関は、携帯電話機から送信された金額を受信し、その金額を利用者の口座に入金してその口座の残高を更新して携帯電話機に送信する。携帯電話機は、携帯電話局から送信された口座の残高を受信して記憶する。したがって、利用者は携帯電話機を財布のように使って決済を行なうことができる。ここでは、クレジット番号などを送信する必要がないので、セキュリティが高い。また、ＩＣカードなどを持ち歩く必要もないので、使い勝手が

APPL-1002
APPLE INC. / Page 653 of 1892

よい。

図面の簡単な説明

図１は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額を通話料と併せて支払う場合の資金移動を示す概略図である。

図２は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額をクレジットカードで支払う場合の資金移動を示す概略図である。

図３は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額をデビットカードで支払う場合の資金移動を示す概略図である。

図４は、この発明の第１の実施の形態に従って仮想口座に入金する前払金額を銀行口座から自動引落しする場合の資金移動を示す概略図である。

図５は、この発明の第１の実施の形態に従って携帯電話機を用いてインターネット上の仮想店舗で決済する方法を示す概略図である。

図６は、この発明の第１の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図７は、図１～図４に示したように仮想口座に前払金を入金するために用いられる、携帯電話機および携帯電話会社のサーバのハードウェア構成を示すブロック図である。

図８は、図１に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図９は、図８に示した携帯電話機の動作中に表示される画面の遷移図である。

図１０は、図２に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１１は、図１０に示した携帯電話機の動作中に表示される画面の遷移図である。

図１２は、図３に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１３は、図１２に示した携帯電話機の動作中に表示される画面の遷移図である。

APPL-1002
APPLE INC. / Page 654 of 1892

図１４は、図４に示した場合における、図７に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図１５は、図１４に示した携帯電話の動作中に表示される画面の遷移図である。

図１６は、この発明の第１の実施の形態に従ってインターネット上の仮想店舗で携帯電話機を用いて決済する場合に用いられる、携帯電話機、携帯電話会社のサーバ、パーソナルコンピュータ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

図１７は、図５に示した場合における図１６に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図１８は、図１７に続くフローチャートである。

図１９は、図１７および図１８に示した携帯電話機の動作中に表示される画面の遷移図である。

図２０は、図６に示した場合に用いられる、携帯電話機、携帯電話会社のサーバ、および実在店舗のＰＯＳ端末のハードウェア構成を示すブロック図である。

図２１は、図２０に示した携帯電話機、実在店舗のＰＯＳ端末、および携帯電話会社のサーバの動作を示すフローチャートである。

図２２は、図２１に続くフローチャートである。

図２３は、図２１および図２２に示した携帯電話機の動作中に表示される画面の遷移図である。

図２４は、携帯電話機のＲＡＭおよびＲＯＭに記憶される情報を示す図である。

図２５は、この発明の第２の実施の形態に従って実在口座から仮想口座に振替える場合の資金移動を示す概略図である。

図２６は、図２５に示したように実在口座から仮想口座への振替に用いられる携帯電話機、携帯電話会社のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図２７は、図２５に示した場合における、図２６に示した携帯電話機、携帯電話会社のサーバ、および金融機関のサーバの動作を示すフローチャートである。

図２８は、図２７に続くフローチャートである。

APPL-1002
APPLE INC. / Page 655 of 1892

図２９は、図２７および図２８に示した携帯電話機の動作中に表示される画面の遷移図である。

図３０は、この発明の第２の実施例に従って携帯電話機を用いてインターネット上の仮想店舗で決済する方法を示す概略図である。

図３１は、図３０に示した場合に用いられるパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、金融機関のサーバ、決済機関のサーバ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

図３２は、図３０に示した場合における、図３１に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、仮想店舗のサーバ、および金融機関サーバの動作を示すフローチャートである。

図３３は、図３２に続くフローチャートである。

図３４は、図３３に続くフローチャートである。

図３５は、図３２～図３４に示した携帯電話機の動作中に表示される画面の遷移図である。

図３６は、この発明の第２の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図３７は、図３６に示した場合に用いられる、携帯電話機、実在店舗のＰＯＳ端末、携帯電話会社のサーバ、金融機関のサーバ、および決済機関のサーバのハードウェア構成を示すブロック図である。

図３８は、図３６に示した場合における、図３７に示した携帯電話機、ＰＯＳ端末、携帯電話会社のサーバ、金融機関のサーバの動作を示すフローチャートである。

図３９は、図３８に続くフローチャートである。

図４０は、図３９に続くフローチャートである。

図４１は、この発明の第３の実施の形態に従ってサービスの利用者情報を登録する方法を示す概略図である。

図４２は、この発明の第３の実施の形態に従って仮想口座に前払金額を入金する場合の資金移動を示す概略図である。

図４３は、この発明の第３の実施の形態に従って携帯電話機を用いてインター

ネット上の仮想店舗で決済する方法を示す概略図である。

図４４は、この発明の第３の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図４５は、この発明の第３の実施の形態に従って決済機関が利用者に対して携帯電話機に蓄積されている未通知データを要求する方法を示す概略図である。

図４６は、この発明の第３の実施の形態に従って携帯電話機を用いてインターネット上の仮想店舗で決済する場合において決済機関が金融機関に対する請求を代行する方法を示す概略図である。

図４７は、図４１に示した利用登録に用いられる、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示すブロック図である。

図４８は、図４１に示した場合における、図４７に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図４９は、図４２に示した仮想口座への資金移動に用いられる、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図５０は、図４２に示した場合における、図４９に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図５１は、図５０に続くフローチャートである。

図５２は、図５１に続くフローチャートである。

図５３は、図４３に示した仮想店舗での決済に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

図５４は、図４３に示した場合における、図５３に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

図５５は、図５４に続くフローチャートである。

図５６は、図５５に続くフローチャートである。

図５７は、図４４に示した実在店舗での決済に用いられる、携帯電話機、ＰＯＳ端末、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示

すブロック図である。

図５８は、図４４に示した場合における、図５７に示した携帯電話機、ＰＯＳ端末、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図５９は、図５８に続くフローチャートである。

図６０は、図５９に続くフローチャートである。

図６１は、図４５に示した未通知データの要求の場合における、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図６２は、図４６に示した請求代行に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

図６３は、図４６に示した場合における、図６２に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

図６４は、図６３に続くフローチャートである。

図６５は、この発明の第４の実施の形態に従う前払方法を示す概略図である。

図６６は、図６５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

図６７は、図６６に続くフローチャートである。

図６８は、この発明の第４の実施の形態に従う第１の送金方法を示す概念図である。

図６９は、図６８に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図７０は、図６９に続くフローチャートである。

図７１は、この発明の第４の実施の形態に従う第２の送金方法を示す概念図です。

図７２は、図７１に示した場合における、パーソナルコンピュータ、携帯電話

APPL-1002
APPLE INC. / Page 658 of 1892

機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図７３は、図７２に続くフローチャートである。

図７４は、この発明の第４の実施の形態に従って、小口決済履歴がない場合におけるワンタイムＩＤの発行方法を示す概念図である。

図７５は、この発明の第４の実施の形態に従って、小口決済履歴がある場合におけるワンタイムＩＤの発行方法を示す概念図である。

図７６は、図７４および図７５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

図７７は、図７６に続くフローチャートである。

図７８は、この発明の第４の実施の形態に従い、ワンタイムＩＤを使用して実在店舗で決済する方法を示す概念図である。

図７９は、図７８に示した場合における、携帯電話機、実在店舗のＰＯＳ端末、および決済機関のサーバの動作を示すフローチャートである。

発明を実施するための最良の形態

以下、この発明の実施の形態を図面を参照して詳しく説明する。図中同一または相当部分には同一符号を付してその説明は繰返さない。

［第１の実施の形態］

１．サービスの概要

この発明の実施の形態は、携帯電話会社が提供する新規サービス（「お財布サービス」と呼び、以下単に「本サービス」という）を実現するためのコンピュータシステムに関するものである。本サービスは、携帯電話機を財布のように使用できるようにするものである。以下、本サービスの概要を説明する。

携帯電話機購入の際、通話料金を引落す銀行口座以外に、クレジットカード番号やキャッシュカード番号などを携帯電話会社に登録する。携帯電話会社は、携帯電話機の利用者ごとに仮想口座を設ける。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社に要請する。携帯電話会社は、予め登録されている銀行口座、クレジットカード番号、キャッシュカ

APPL-1002
APPLE INC. / Page 659 of 1892

ード番号などを用い、利用者に対して前払金の請求を行なう。前払金の支払方法は、利用者が選択することができる。前払金の請求後、携帯電話会社は、仮想口座に前払金を入金したうえで仮想口座の残高を携帯電話機に送信する。携帯電話機は、送信された仮想口座の残高を記憶する。利用者は、この携帯電話機を財布代わりに使ってインターネット上の仮想店舗や実在店舗で決済を行なう。店舗は、携帯電話会社に対して請求を行なう。

２．前払金の支払方法

次に、４通りの前払金の支払方法について説明する。

２－１．通話料と併せて支払う場合

図１は、前払金を通話料と併せて支払う場合の資金移動を示す概略図である。図１に示すように、携帯電話会社（携帯電話局）１０には、個人情報データベース１１が設けられている。個人情報データベース１１には、各利用者１２の個人情報が登録されている。具体的には、前払金（携帯電話会社にとっては前受金）を蓄積するための仮想口座１１０が設けられ、携帯電話機１３の電話番号の他、電子メールアドレス、パスワード、利用状況、キーコード、口座番号、クレジットカード番号、デビットカード番号などが予め登録されている。

まず、利用者１２は携帯電話機１３を用いて所望の前払金額とその支払方法（ここでは「通話料に加算」）とを携帯電話会社１０に送信する。このとき、携帯電話機１３の電話番号も併せて送信する。

携帯電話会社１０は、送信された携帯電話番号に基づいて個人情報データベース１１を検索し、利用者１２の仮想口座１１０の利用状況を照会する。利用者１２に問題がなければ（利用状況が「ＯＫ」であれば）、携帯電話会社１０は送信された前払金額を仮想口座１１０の前受残高に加算し、更新した最新の前受残高を送信する。一方、利用者１２の支払いが滞っていたり、本サービスの利用が停止されている場合、利用状況は「ＮＧ」となっている。この場合、携帯電話会社１０は携帯電話機１３を通じて本サービスを利用できない旨を利用者１２に通知する。

上記のように利用者１２が支払方法として「通話料に加算」を選択した場合、携帯電話会社１０は、基本料金と通話料金の請求書１４と併せて本サービスの利

用明細書１５を利用者１２に送付する。

携帯電話会社１０は、個人情報データベース１１に登録されている口座番号に基づいて利用者１２の取引銀行１７に利用料金の引落しを依頼する。これに応じて銀行１７は、利用者１２の口座１６から、銀行１８に開設されている携帯電話会社１０の口座１９に資金を振替える。

２－２．クレジットカードで支払う場合

図２は、前払金をクレジットカードで支払う場合の資金移動を示す概略図である。この場合、図２に示すように、利用者１２は携帯電話機１３を用いて前払金額とその支払方法（ここでは「クレジットカード」）とを携帯電話会社１０に送信する。

携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されているクレジットカード番号に基づいて信販会社２０に承認を依頼する。信販会社２０は、承認できる場合はその旨を携帯電話会社１０に通知する。これに応じて、携帯電話会社１０は仮想口座１１０の前受残高を更新し、その最新の前受残高を携帯電話機１３に送信する。一方、承認できない場合は、信販会社２０はその旨を携帯電話会社１０に通知する。これに応じて、携帯電話会社１０は前受残高を更新することなく、クレジットカードによる支払いができない旨を利用者１２に通知する。

支払いを承認した場合、信販会社２０は、利用者１２が所望した前払金額を携帯電話会社１０の口座１９に振込む。次いで信販会社２０は、銀行１７に対して利用者１２の口座１６から前払金額を引落すように依頼する。これに応じて銀行１７は、利用者１２の口座１６から信販会社２０に資金を振替える。

２－３．デビットカードで支払う場合

図３は、前払金をデビットカードで支払う場合の資金移動を示す概略図である。この場合、図３に示すように、利用者１２は携帯電話機１３を用いて前払金額とその決済方法（ここでは「デビットカード」）とを携帯電話会社１０に送信する。

携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されているデビットカード番号に基づいてそのデビットカードを発行した銀行１７に資金の振替えを依頼する。振替え依頼を承認した場合、銀行１７はその振替えデ

ータをクリアリングセンター２１に送信するとともに、振替えの完了を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新し、その最新の前受残高を携帯電話機１３に送信する。一方、銀行１７が振替え依頼を承認しない場合、振替えできない旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新することなく、デビットカードで支払いできない旨を利用者１２に通知する。

クリアリングセンター２１は、銀行１７の他、多数の銀行から送信された振替えデータに基づいて振替えの相殺および集計を行ない、銀行間の決済尻データを決済銀行２２に送信する。これに応じて決済銀行２２は、銀行１７から加盟店銀行２３に資金を振替える。これに応じて加盟店銀行２３は、その資金を携帯電話会社１０の口座１９に入金する。

２－４．自動引落しで支払う場合

図４は、前受金を銀行口座から自動引落しで支払う場合の資金移動を示す概略図である。この場合、図４に示すように、利用者１２は携帯電話機１３を用いて前払金額とその支払方法（ここでは「自動引落」）とを携帯電話会社１０に送信する。携帯電話会社１０は、利用者１２の利用状況に問題がなければ、予め登録されている口座番号に基づいて銀行１７に資金の引落しを依頼する。引落しが可能な場合、銀行１７はその旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、前受残高を更新し、最新の前受残高を携帯電話機１３に送信する。引落しが不可能な場合、銀行１７はその旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、支払いできない旨を利用者１２に通知する。携帯電話会社１０から引落し依頼を受けた銀行１７は直ちに、利用者１２の口座１６から携帯電話会社１０の口座１９に資金を振替える。これとは別に、利用明細書１５は請求書１４と併せて利用者１２に送付される。

３．決済

次に、携帯電話機１３を使って上述した前払金で決済を行なう方法について説明する。

３－１．インターネット上の仮想店舗での決済

図５は、インターネット上の仮想店舗で携帯電話機を使って決済する方法を示

す概略図である。図５に示すように、まず、利用者１２は携帯電話機１３またはパーソナルコンピュータ４０でインターネット上の仮想店舗２４に商品やサービスを注文し、その決済方法（ここでは「携帯電話決済」）を選択する。パーソナルコンピュータ４０を用いる場合、利用者１２は携帯電話機１３の電話番号をパーソナルコンピュータ４０に手で入力し、インターネット６０を通じて仮想店舗２４に送信する。

注文を受けた仮想店舗２４は、送信された携帯電話番号に基づいて携帯電話会社１０に決済金額の請求を依頼する。

請求依頼を受けた携帯電話会社１０は、利用者１２の利用状況に問題があれば本サービスが利用できない旨を仮想店舗２４に通知する。これに応じて仮想店舗２４は、本サービスが利用できない旨を利用者１２に通知する。利用者１２の利用状況に問題がなければ、携帯電話会社１０は予め登録されている利用者１２の電子メールアドレスに基づいて利用者１２の携帯電話機１３に電子メールで電子請求書を送信する。電子請求書は、仮想口座１１０からの支払いを利用者１２に確認するためのものである。

また、電子請求書を受取った利用者１２は、その決済を承認するか否かを選択する。利用者１２が決済を承認した場合、電子請求書を受信した携帯電話機１３は、前払残高を検証し、前払残高が決済金額を下回っている場合、携帯電話機１３は残高不足として決済ができない旨を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、残高が不足しているから決済できない旨を仮想店舗２４を通じて利用者１２に通知する。利用者１２が決済を取消しまたは拒否した場合、決済取消しまたは決済拒否を携帯電話会社１０に通知する。これに応じて携帯電話会社１０は、決済が取消しまたは拒否されたから決済できない旨を仮想店舗２４に通知する。これに応じて仮想店舗２４は、決済できない旨を利用者１２に通知する。

また、利用者１２が決済を承認した場合において、前払残高の検証の結果、決済金額が前払残高以内のとき、その決済を了承する旨を携帯電話会社１０に通知する。このとき、予め携帯電話会社１０に登録されているパスワード、携帯電話番号、キーコードなどを併せて送信する。携帯電話会社１０は、送信された携帯

電話番号に基づいて個人情報データベース１１を検索し、送信されたパスワードおよびキーコードが予め登録されているパスワードおよびキーコードとそれぞれ一致するか否かを判別する。キーコードが一致しない場合、携帯電話会社１０はキーコードが異常であるから本サービスを利用できない旨を利用者１２に通知するとともに、決済できない旨を仮想店舗２４を通じて利用者１２に通知する。両者とも一致する場合、携帯電話会社１０は仮想口座１１０の前受残高から決済金額を減算して前受残高を更新するとともに、その更新した前受残高を携帯電話機１３に送信する。これに応じて携帯電話機１３は内部の前受残高を更新する。また、携帯電話会社１０は決済完了を仮想店舗２４に通知する。これに応じて仮想店舗２４は決済完了を利用者１２に通知する。

その後、仮想店舗２４は注文を受けた商品を利用者１２に届けたり、注文を受けたサービスを利用者１２に提供する。携帯電話会社１０は、上記決済金額を仮想店舗２４に入金する。仮想店舗２４は、本サービスを利用した手数料を携帯電話会社１０に支払う。

３－２．実在店舗での決済

図６は、実在店舗で携帯電話機を使って決済する方法を示す概略図である。図６に示すように、実在店舗において、利用者１２は携帯電話機１３をＰＯＳ端末２７に接続された読取装置２７０にセットする。店員は商品の金額をＰＯＳ端末２７に打ち込み、決済金額を計算する。この決済金額はＰＯＳ端末２７から読取装置２７０を通じて携帯電話機１３に送信される。携帯電話機１３は、内部に記憶されている残高と決済金額とを比較し、決済が不可能であればエラーをＰＯＳ端末２７に送信する。一方、決済が可能であれば、携帯電話機１３は携帯電話番号とキーコードとをＰＯＳ端末２７に送信する。携帯電話番号は、ＰＯＳ端末２７に手で直接入力することはできない。

携帯電話番号とキーコードとを受信したＰＯＳ端末２７は決済を完了して、その旨を携帯電話機１３に通知する。決済完了を受けて、携帯電話機１３はその決済金額を内部メモリに記憶し、決済モードがオフになる。その後、利用者１２は携帯電話機１３を読取装置２７０から取り除く。

次に、決済金額とともに携帯電話番号およびキーコードを携帯電話会社１０に

送信する。これに応じて携帯電話会社１０は、仮想口座１１０の前受残高から決済金額を減算して前受残高を更新するとともに、決済完了をＰＯＳ端末２７に通知する。

４．ハードウェア構成

図７は、携帯電話機１３、および携帯電話会社１０に設置されるサーバコンピュータ（以下、単にサーバという）３０のハードウェア構成を示すブロック図である。

図７に示すように、携帯電話機１３は、ＣＰＵからなるデータ処理部１３１と、ＲＡＭ１３２と、ＥＥＰＲＯＭのようなＲＯＭ１３３と、アンテナ１３４と、送受信部１３５と、テンキーやカーソルキーのような入力装置１３６と、液晶ディスプレイのような表示装置１３７と、バッテリ１３８と、インターフェイス（Ｉ／Ｆ）部１３９とを備える。この携帯電話機１３は電源アダプタ１４０に装着され、電源アダプタ１４０からＩ／Ｆ部１３９を通じてバッテリ１３８に電流が供給され、バッテリ１３８が充電される。データ処理部１３１は、ＲＡＭ１３２、ＲＯＭ１３３、送受信部１３５、入力装置１３６、表示装置１３７およびＩ／Ｆ部１３９を用いて通常の携帯電話機能を実行する他、後述する決済機能を実行する。

携帯電話会社１０に設置されているサーバ３０は、ＣＰＵからなるデータ処理部３０１と、データベース３０２とを備える。データベース３０２は、個人情報データベース１１と、利用履歴データベース２８と、決済履歴データベース２９とを含む。データ処理部３０１はデータベース３０２を用いて後述する決済機能を実行する。データ処理部３０１は無線基地局３０３に接続されている。無線基地局３０３のアンテナ３０４と携帯電話機１３のアンテナ１３４との間で電波が送受信される。利用履歴データベース２８は、携帯電話機１３とのデータの取引内容を記録するためのログファイルである。具体的には、仮想口座１１０の入出金日時、入出金額、残高などが記録される。決済履歴データベース２９は、店舗とのデータの取引内容を記録するためのログファイルである。具体的には、決済日時、決済金額などが記録される。

５．前払い時の処理動作

５－１．通話料と併せて支払う場合

図８は、図１に示した前払金を通話料と併せて支払う場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図９は、この場合に携帯電話機１３の表示装置１３７に表示される表示画面の遷移図である。

まず、携帯電話機１３のデータ処理部１３１は、表示装置１３７上に図９に示した画面Ｄ１を表示し、利用者１２に対してパスワードの入力を促す。利用者１２が入力装置１３６を操作してパスワードを入力すると、入力装置１３６はその入力されたパスワードをデータ処理部１３１に与える（Ｓ１０１）。

続いて、データ処理部１３１はその入力されたパスワードをＲＡＭ１３２またはＲＯＭ１３３に予め登録されているパスワードと比較することにより入力されたパスワードの検証を行なう（Ｓ１０２）。入力されたパスワードが誤っている場合、データ処理部１３１は表示装置１３７上に図９に示した画面Ｄ２を表示する（Ｓ１０３）。一方、入力されたパスワードが正しい場合、データ処理部１３１は表示装置１３７上に図９にした画面Ｄ３を表示し、利用者１２に対し、「①お金を払う」、「②お財布の中を見る」、「③お財布にお金を入れる」の中から１つを選択するよう促す。利用者１２が入力装置１３６を操作し、「③お財布にお金を入れる」を選択すると、データ処理部１３１は表示装置１３７上に画面Ｄ４を表示し、利用者１２に対して前払金額の入力を促す。このとき、未通知データ（詳細は後述する）がない場合はＲＡＭ１３２に記憶されている前払残高を現在の残高として表示し、未通知データがある場合はＲＡＭ１３２に記憶されている前払残高から未通知の決済金額を減算して真の前払残高を計算し、それを現在の残高として表示する。利用者１２が入力装置１３６を操作して所望の前払金額を入力すると、入力装置１３６がその入力された前払金額をデータ処理部１３１に与える（Ｓ１０４）。

続いて、データ処理部１３１は表示装置１３７上に画面Ｄ５を表示し、利用者１２に対して前払金額の支払方法を選択するよう促す。利用者１２が入力装置１３６を操作すると、「通話料に加算」という支払方法の他、「クレジット」、「デビットカード」、「自動引落」といういくつかの支払方法が表示される。ここでは利用者１２が「通話料に加算」という支払方法を選択するものとする。こ

APPL-1002
APPLE INC. / Page 666 of 1892

れに応じて、入力装置１３６は「通話料に加算」という支払方法の選択をデータ処理部１３１に与える（Ｓ１０５）。

続いて、データ処理部１３１は選択された支払方法および入力された前払金額を送受信部１３５に与え、送受信部１３５はこれらを携帯電話会社１０に送信する（Ｓ１０６）。このとき、ＲＯＭ１３３に予め記憶されている利用者１２に固有の携帯電話番号と、ＲＯＭ１３３に予め記憶されている携帯電話機１３に固有のキーコードと、ＲＡＭ１３２に記憶されている未通知データとを併せて送信する。携帯電話番号は、携帯電話会社１０が携帯電話機１３を販売する際にＥＥＰＲＯＭのようなＲＯＭ１３３に予めプログラムする。キーコードは、携帯電話機メーカが携帯電話機を製造する際に製造番号や各携帯電話機固有の管理番号（サブスクライバＩＤ（識別子）、機体ＩＤ、端末ＩＤなどと呼ばれる）などをＥＥＰＲＯＭのようなＲＯＭ１３３に予めプログラムする。したがって、携帯電話番号は利用者１２に固有のもので、携帯電話機１３を買い換えた場合でも同じ携帯電話番号を登録することができる。ただし、利用者１２自身は携帯電話番号を書き換えることはできず、利用者１２の依頼に応じて携帯電話会社１０が書き換えることになる。これに対し、キーコードは携帯電話機１３に固有のものである。キーコードに製造番号を用いた場合、利用者１２はもちろん、携帯電話会社１０さえも書き換えることができない。キーコードに上述したサブスクライバＩＤのような管理番号を用いた場合、携帯電話会社１０は書き換えることができるが、利用者１２は書き換えることができない。

続いて、データ処理部１３１はこれまでの処理が正常に終了したか否かを判別し（Ｓ１０７）、正常に終了していない場合はその旨を表示装置１３７に表示し（Ｓ１０８）、接続を切断する（Ｓ１０９）。一方、正常に終了した場合は異常終了の表示をすることなく接続を一旦切断する（Ｓ１０９）。

一方、携帯電話会社１０に設置されているサーバ３０において、データ処理部３０１は、携帯電話機１３から送信された前払金額、支払方法、携帯電話番号およびキーコードを無線基地局３０３を通じて受信する（Ｓ２０１）。

続いて、データ処理部３０１は受信した携帯電話番号に基づいて個人情報データベース１１を検索する（Ｓ２０２）。

続いて、データ処理部３０１は受信したキーコードを検索した個人情報データベース１１のキーコードと比較し、キーコードが一致するか否か確認する（Ｓ２０３）。キーコードが一致した場合、データ処理部３０１は個人情報データベース１１の利用状況を確認し、問題があるか否か判別する（Ｓ２０４）。上記ステップＳ２０２でキーコードが一致しない場合、またはこのステップＳ２０４で利用状況に問題がある場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に送信する（Ｓ２０５）。

携帯電話機１３においては、送受信部１３５が携帯電話機１３から送信された本サービス利用不可能の情報を受信する（Ｓ１１０）

続いて、データ処理部１３１は図９に示した画面Ｄ６を表示装置１３７上に表示し、本サービスを利用できない旨を利用者１２に通知する（Ｓ１１１）。そして、データ処理部１３１は表示装置１３７上に異常に終了した旨を表示する（Ｓ１１２）。

一方、上記ステップＳ２０４で利用状況に問題がなければ、利用履歴データベース２８を更新する（Ｓ２０６）。具体的には、現在の日時と、今回の前受金額（利用者１２にとっては前払金額）と、現在の前受残高と、未通知データ（未通知の決済金額）とを利用履歴データベース２８に記録する。

続いて、データ処理部３０１は現在の前受残高を携帯電話機１３に送信する（Ｓ２０７）。

続いて、データ処理部３０１はこの前受金額について請求データを作成する（Ｓ２０８）。

続いて、データ処理部３０１は作成した請求データを毎月一括して通話料に加算し、図１に示すように請求書１４とともに本サービスの利用明細書１５を発行する。

以降の処理は既存の処理と同じで、利用者１２の個人情報データベース１１に登録されている口座番号に基づき利用者１２の取引銀行１７に対して料金の引落しを依頼する（Ｓ２０９）。これに応じて、本サービスの利用料金が通話料と併せて利用者の口座１６から携帯電話会社の口座１９に振替えられる。

携帯電話機１３においては、上記ステップＳ２０７でサーバ３０から送信され

た前受残高を送受信部１３５が受信する（Ｓ１１３）。

続いて、データ処理部１３１は受信した前受残高を前払残高としてＲＡＭ１３２に格納し、これにより前受残高を更新する（Ｓ１１６）。

続いて、データ処理部１３１は図９に示した画面Ｄ７を表示装置１３７に表示する（Ｓ１１７）。具体的には、これまでの前払処理が完了した旨と現在の前払残高とを表示する。

５－２．クレジットカードで支払う場合

図１０は、図２に示した前払金額をクレジットカードで支払う場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１１は、この場合に携帯電話機１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり前払金額をクレジットカードで支払う場合は、図１１に示した画面Ｄ５で利用者１２は「クレジット（一括）」を選択する。これに応じて、入力装置１３６はクレジットカードによる支払いという支払方法の選択をデータ処理部１３１に与える（図１０，Ｓ１０５）。

また、携帯電話会社１０のサーバ３０においては、利用状況に問題がない場合、個人情報データベース１１に予め登録されているクレジットカード番号に基づいて信販会社２０に利用者１２の与信照会を行なう（Ｓ２１０）。

続いて、データ処理部３０１は信販会社２０からの返信に基づいて信販会社２０がクレジットカードによる支払いを承認したか否かを判別する（Ｓ２１１）。

非承認の場合、データ処理部３０１は支払できない旨を携帯電話機１３に送信する（Ｓ２１２）。承認の場合は、利用履歴データベース２８を更新する（Ｓ２０５）。

一方、携帯電話機１３においては、送受信部１３５がサーバ３０からクレジットカードによる支払いは不可能な旨を受信した場合、図１２に示した画面Ｄ８を表示装置１３７に表示し、クレジットカードによる支払いが不可能な旨を利用者１２に通知する（Ｓ１２０）。

５－３．デビットカードで支払う場合

図１２は、前払金額をデビットカードで支払う場合の携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１３は、この場合に携帯電話機

１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり前払金額をデビットカードで支払う場合、図１３に示した表示画面Ｄ５において利用者１２は「デビットカード」を選択する。これに応じて、入力装置１３６はその選択情報をデータ処理部１３１に与える（Ｓ１０５）。

一方、携帯電話会社１０のサーバ３０においては、利用状況に問題がない場合、データ処理部３０１は個人情報データベース１１に予め登録されているデビットカード番号に基づいてそのデビットカードの発行銀行１７に引落し（承認）依頼を送信する（Ｓ２２０）。これに応じて、既存のデビットカード処理が実行される（Ｓ２２１）。

続いて、データ処理部３０１はデビットカードの発行銀行１７から送信された振替え結果に基づいて振替えが完了したか否かを判別する（Ｓ２２２）。振替えができなかった場合、データ処理部３０１はその旨を携帯電話機１３に送信する（Ｓ２１２）。

これに応じて携帯電話機１３のデータ処理部１３１は、図１３に示した画面Ｄ９を表示装置１３７に表示し（Ｓ１２０）、デビットカードによる支払いができない旨を利用者１２に通知する。

５－４．自動引落で即時支払う場合

図１４は、図４に示した前払金額を利用者の口座１６から自動的に引落す場合における携帯電話機１３およびサーバ３０の動作を示すフローチャートである。図１５は、この場合に携帯電話機１３の表示装置１３７に表示される画面の遷移図である。

上記と異なり自動引落しの場合、図１５に示した画面Ｄ５で利用者１２は「自動引落」を選択し、この利用者１２の操作に応じて入力装置１３６はデータ処理部１３１にその選択情報を与える（Ｓ１０５）。

一方、サーバ３０においては、利用状況に問題がない場合、データ処理部３０１は受信した前払金額が引落し可能か否かを利用者１２の取引銀行１７に照会する（Ｓ２３０）。

続いて、データ処理部３０１は銀行１７から返信された照会結果に基づいて引落しが可能か否かを判別する（Ｓ２３１）。引落しが不可能な場合、データ処理

APPL-1002
APPLE INC. / Page 670 of 1892

部３０１はその旨を携帯電話機１３に送信する（Ｓ２３２）。

これに応じて携帯電話機１３のデータ処理部１３１は、図１５に示した画面Ｄ１０を表示し（Ｓ１２０）、利用者の口座１６からは所望の前払金額を引落すことができない旨を利用者１２に通知する。

一方、引落しが可能な場合、携帯電話会社１０は既存の方法で銀行１７に引落しを依頼する（Ｓ２２３）。

６．決済時の処理動作

次に、携帯電話機１３を用いてインターネット上の仮想店舗および実在店舗で決済を行なう場合の動作について説明する。

６－１．仮想店舗で決済する場合

図１６は、仮想店舗で決済を行なう場合に用いられる利用者のパーソナルコンピュータ（ＰＣ）４０および携帯電話機１３、携帯電話会社のサーバ３０、ならびに仮想店舗のサーバコンピュータ（以下、単にサーバという）５０のハードウェア構成を示すブロック図である。

図１６に示すように、利用者１２のパーソナルコンピュータ４０は、ＣＰＵのようなデータ処理部４０１と、ＲＯＭやＲＡＭのようなメモリ４０２と、ハードディスク（ＨＤ）４０３と、モデム４０４と、キーボードやマウスのような入力装置４０５と、ＣＲＴディスプレイや液晶ディスプレイのような表示装置４０６とを備える。仮想店舗２４のサーバ５０も同様に、データ処理部５０１と、メモリ５０２と、ハードディスク５０３と、モデム５０４と、入力装置５０５と、表示装置５０６とを備える。パーソナルコンピュータ４０はモデム４０４を通じてインターネット６０に接続される。サーバ５０もモデム５０４を通じてインターネット６０に接続される。携帯電話会社１０のサーバ３０もモデム３０３を通じてインターネット６０に接続される。

図１７および図１８は、図１６に示したパーソナルコンピュータ４０、携帯電話機１３、サーバ３０および５０の動作を示すフローチャートである。

利用者１２はパーソナルコンピュータ４０の入力装置４０５を操作して仮想店舗２４に商品やサービスの注文を行ない、その決済方法として携帯電話決済を選択する。これに応じて、パーソナルコンピュータ４０のデータ処理部４０１は入

APPL-1002
APPLE INC. / Page 671 of 1892

力された注文情報および携帯電話番号をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ３０１）。

サーバ５０のデータ処理部５０１は、送信された注文情報および携帯電話番号を受信する（Ｓ６０１）。

続いて、データ処理部５０１は、店舗名、決済金額、携帯電話番号などの請求情報をインターネット６０を通じて携帯電話会社１０のサーバ３０に送信することにより、携帯電話会社１０に利用者１２の決済金額を請求する（Ｓ６０２）。

サーバ３０のデータ処理部３０１は、送信された請求情報を受信する（Ｓ５０１）。

続いて、データ処理部３０１は受信した携帯電話番号に基づいて個人情報データベース１１を検索する（Ｓ５０２）。

続いて、データ処理部３０１は検索した利用者１２の個人情報の中から利用状況を照会し、問題がないか否か確認する（Ｓ５０３）。問題がある場合、データ処理部３０１は本サービス利用不可の情報をサーバ５０に送信する。これにより、本サービスを利用できない旨を仮想店舗２４に通知する（Ｓ５０４）。一方、利用状況に問題がない場合、データ処理部３０１は検索した個人情報の中から利用者１２の電子メールアドレスを特定し、電子メールで請求データを携帯電話機１３に送信する（Ｓ５０５）。これは、携帯電話会社１０が仮想店舗２４に代わって利用者１２に請求書を発行することを意味する。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０のサーバ３０から送信された請求データを受信する（Ｓ４０１）。

利用者１２が携帯電話機１３の入力装置１３６を操作して「受信メール一覧」を選択すると、携帯電話機１３のデータ処理部１３１は図１９に示した画面Ｄ１１を表示装置１３７上に表示する。利用者１２が入力装置１３６を操作して請求データの電子メールを選択すると、データ処理部１３１は画面Ｄ１２を表示装置１３７上に表示する。これは電子請求書であり、注文日、注文者（通常は利用者１２と同じ）、請求者（通常は仮想店舗２４と同じ）、請求額（通常は決済金額と同じ）が表示されている。

利用者１２が請求内容を確認し、同意できれば「支払」を選択し、同意できな

APPL-1002
APPLE INC. / Page 672 of 1892

ければ「拒否」を選択する。携帯電話機１３の入力装置１３６はこのような利用者１２の操作に応じて選択情報をデータ処理部１３１に入力する。データ処理部１３１は入力された選択情報に基づいて決済が承認されたか否かを判別する（Ｓ４０２）。決済が承認されなかった場合、送受信部１３５は決済取消・拒否の情報を携帯電話機１０のサーバ３０に送信する（Ｓ４０３）。この場合、データ処理部１３１は、図１９に示した画面Ｄ１３を表示装置１３７上に表示する（Ｓ４０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された決済取消・拒否の情報を受信し（Ｓ５０６）、さらにその情報を仮想店舗２４のサーバ５０に送信する（Ｓ５０７）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された決済取消・拒否の情報を受信する（Ｓ６０５）。

続いて、データ処理部５０１は受信した決済取消・拒否の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信し、これにより仮想店舗２４は利用者１２に決済が取消しまたは拒否された旨を利用者１２に通知する（Ｓ６０６）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２４のサーバ５０から送信された決済取消・拒否の情報を受信し（Ｓ３０４）、決済が取消しまたは拒否された旨を表示装置４０６上に表示する。

上記ステップＳ４０２で決済が承認された場合、携帯電話機１３のデータ処理部１３１は、ＲＡＭ１３２内に未通知データ（電波圏外の店舗で決済したために携帯電話会社１０に未だ通知できていない決済日時、決済金額などで、その詳細は後述する。）が存在しないか否かを判別する（Ｓ４０５）。未通知データがある場合、データ処理部１３１は未通知の決済金額を合計して累計未通知金額を計算し（Ｓ４０６）、続いてＲＡＭ１３２に記憶されている前払残高から累計未通知金額を減算して現時点における真の前払金額を計算する（Ｓ４０７）。

上記ステップＳ４０５で未通知データがない場合、または上記ステップＳ４０７の後、データ処理部１３１は前払残高を検証し、決済金額が前受残高以内か否かを判別する（Ｓ４０８）。決済金額が前受残高を超えている場合、データ処理

部１３１は図１９に示した画面Ｄ１４を表示装置１３７上に表示して残高不足を利用者１２に通知し（Ｓ４０９）、続いて残高不足の情報を電波で携帯電話会社１０のサーバ３０に送信する（Ｓ４１０）。

これに応じて携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された残高不足の情報を受信し（Ｓ５０８）、続いてこの残高不足の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ５０９）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された残高不足の情報を受信し（Ｓ６０７）、続いてこの残高不足の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信する（Ｓ６０８）。利用者１２のパーソナルコンピュータ４０はこの残高不足の情報を受信し、その旨を表示装置４０６上に表示する（Ｓ３０５）。

一方、携帯電話機１３において、上記ステップＳ４０８で決済金額が前払残高以内の場合、データ処理部１３１は図１９に示した画面Ｄ１を表示し、利用者１２にパスワードの入力を促す。利用者１２がパスワードを入力すると、入力装置１３６は入力されたパスワードをデータ処理部１３１に与える（Ｓ４１１）。

続いて、送受信部１３５は、決済承認の情報および未通知データを携帯電話会社１０のサーバ３０に電波で送信する（Ｓ４１２）。具体的には、携帯電話機１３の電話番号、ＲＯＭ１３３に予めハード的に登録されているキーコード、上記ステップＳ４１１で入力されたパスワード、未通知の決済金額を送信する。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された決済承認の情報を受信する（Ｓ５１０）。

続いて、データ処理部３０１は個人情報データベース１１を検索し、受信した携帯電話番号に基づいて利用者１２の個人情報を特定する。データ処理部３０１はさらに、受信したキーコードを利用者１２の個人情報として予め登録されているキーコードと比較し、キーコードが一致するか否かを判別する（Ｓ５１１）。キーコードが一致した場合、データ処理部３０１は、受信したパスワードを利用者１２の個人情報として予め登録されているパスワードと比較し、パスワードが

一致するか否かを判別する（Ｓ５１２）。

キーコードが一致しない場合、またはパスワードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信し、これにより携帯電話会社１０は利用者１２に本サービスが利用できない旨を通知する（Ｓ５１３）。

利用者の携帯電話機１３においては、送受信部１３５が携帯電話会社１０のサーバ３０から送信された本サービス利用不可の情報を受信する（Ｓ４１３）。

続いて、データ処理部１３１は本サービスが利用できない旨を表示装置１３７上に表示する（Ｓ４１４）。

続いて、データ処理部１３１は本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ４１５）。

一方、携帯電話会社１０の携帯電話機１３において、データ処理部３０１は決済不可の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信する（Ｓ５１４）。

仮想店舗２４のサーバ５０においては、データ処理部５０１が携帯電話会社１０のサーバ３０から送信された決済不可の情報を受信する（Ｓ６０９）。

これに応じて、データ処理部５０１は決済不可の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信し、これにより仮想店舗２４は利用者１２に決済ができない旨を通知する（Ｓ６１０）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２１のサーバ５０から送信された決済不可の情報を受信し（Ｓ３０６）、決済ができない旨を表示装置４０６上に表示する。

一方、携帯電話会社１０のサーバ３０においては、上記ステップＳ５１２でパスワードが一致した場合、データ処理部３０１は利用履歴データベース２８を更新し、利用者１２の仮想口座１１０の前受残高を更新する（Ｓ５１５）。利用履歴データベース２８には具体的には、決済日時、決済金額などを記録する。

続いて、データ処理部３０１は更新した前受残高を電波で携帯電話機１３に送信する（Ｓ５１６）。

携帯電話機１３においては、データ処理部１３１が携帯電話会社１０のサーバ

３０から送信された仮想口座１１０の前受残高を受信する（Ｓ４１６）。

続いて、データ処理部１３１は受信した仮想口座の前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらにＲＡＭ１３２に記憶されている未通知データをクリアする（Ｓ４１７）。これにより、携帯電話機１３内の前払残高と携帯電話会社内の仮想口座１１０の前受残高とが同期する。

そして、データ処理部１３１は図１９に示した画面Ｄ１５を表示装置１３７上に表示し、決済が完了した旨を利用者１２に通知する。

携帯電話会社１０のサーバ３０においては、上記ステップＳ５１６の後、決済完了の情報をインターネット６０を通じて仮想店舗２４のサーバ５０に送信し、これにより携帯電話会社１０は決済が完了した旨を仮想店舗２４に通知する（Ｓ５１７）。そして、携帯電話会社１０は既存の方法で仮想店舗２４に決済金額を支払う（Ｓ５１８）。

一方、仮想店舗２４のサーバ５０においては、データ処理部５０１は携帯電話会社１０のサーバ３０から送信された決済完了の情報を受信する（Ｓ６１１）。

続いて、データ処理部５０１は受注明細および決済完了の情報をインターネット６０を通じて利用者１２のパーソナルコンピュータ４０に送信する（Ｓ６１２）。

利用者１２のパーソナルコンピュータ４０においては、データ処理部４０１が仮想店舗２４のサーバ５０から送信された受注明細および決済完了の情報を受信する（Ｓ３０７）。

６－２．実在店舗で決済する場合

図２０は、実在店舗で決済する場合に用いられる携帯電話機１３、ＰＯＳ端末３７およびサーバ３０のハードウェア構成を示すブロック図である。

図２０に示すように、ＰＯＳ端末２７も同様に、データ処理部２７１と、ＲＡＭ２７２と、ハードディスク２７３と、入力装置２７４と、表示装置２７５と、インターフェイス（Ｉ／Ｆ）部２７６とを備える。決済時に携帯電話機１３がセットされる読取装置２７０はインターフェイス２７６に接続される。商品バーコードを読取るためのスキャナもインターフェイス部２７６に接続される。現金引出し部２７８もインターフェイス部２７６に接続される。

APPL-1002
APPLE INC. / Page 676 of 1892

図２１および図２２は、図６に示したように実在店舗で決済する場合における携帯電話機１３、ＰＯＳ端末２７およびサーバ３０の動作を示すフローチャートである。

まず利用者１２は実在店舗２６で買物する前に、図２３に示した画面Ｄ１で携帯電話機１３の入力装置１３６を操作してパスワードを入力し、これに応じて入力装置１３６は入力されたパスワードをデータ処理部１３１に与える（Ｓ７０１）。

続いて、データ処理部１３１は入力されたパスワードを、図２４に示すようにＲＡＭ１３２に予め登録されているパスワードと比較し、パスワードの検証を行なう（Ｓ７０２）。パスワードが一致しない場合、データ処理部１３１は図２３に示した画面Ｄ２を表示装置１３７上に表示する（Ｓ７０３）。

一方、パスワードが一致した場合、データ処理部１３１は図２３に示したメニュー画面Ｄ３を表示する。利用者１２が「①お金を払う」を選択すると、データ処理部１３１は未通知データがあるか否かを判別する（Ｓ７０４）。未通知データは、電波圏外の店舗で決済した場合に、その決済金額、決済日時、決済店舗などが図２４に示すようにＲＡＭ１３２に累積的に格納されたものである。未通知データがある場合、データ処理部１３１は電波圏内か否かを判別し（Ｓ７０５）、電波圏内の場合、送受信部１３５は電波で携帯電話会社１０のサーバ３０に未通知データを図２４に示すようにＲＯＭ１３３に予め登録されたキーコードとともに送信する（Ｓ７０６）。電波圏外の場合、ＲＡＭ１３２に記憶されている未通知の決済金額を合計して累計未通知金額を計算し（Ｓ７０７）、続いてＲＡＭ１３２に記憶されている前払残高からその累計未通知金額を減算し、現在の真の前払残高を計算する（Ｓ７０８）。携帯電話機１３内の前払残高は、携帯電話会社１０から仮想口座１１０の前受残高が送信されて来ない限り更新されない。したがって、電波圏外の実在店舗で連続して携帯電話機１３で決済を行なった場合などは、その各決済金額を未通知データとしてＲＡＭ１３２に記憶しておく。

一方、携帯電話会社１０のサーバ３０においては、上記ステップＳ７０６で利用者１２の携帯電話機１３から送信された未通知データをデータ処理部３０１が受信する（Ｓ９０１）。

APPL-1002
APPLE INC. / Page 677 of 1892

続いて、データ処理部３０１は、携帯電話機１３から送信されたキーコードを、個人情報データベース１１に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する（Ｓ９０２）。キーコードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信し、これにより携帯電話会社１０は利用者１２に本サービスが利用できない旨を通知する（Ｓ９０３）。キーコードが一致する場合、データ処理部３０１は受信した未通知データに基づいて利用履歴データベース２８を更新し、仮想口座１１０の前受残高を更新する（Ｓ９０４）。続いて、データ処理部３０１は更新した最新の前受残高を携帯端末機１３に送信する（Ｓ９０５）。

携帯電話機１３においては、上記ステップＳ９０３で携帯電話会社１０のサーバ３０から送信された本サービス利用不可の情報を送受信部１３５が受信する（Ｓ７０９）。続いて、データ処理部１３１は本サービスが利用できない旨を表示装置１３７上に表示し（Ｓ７１０）、さらに本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ７１１）。

また、上記ステップＳ９０５で携帯電話会社１０のサーバ３０から送信された前受残高を送受信部１３５が受信する（Ｓ７１２）。続いて、データ処理部１３１は受信した前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらに未通知データをクリアする（Ｓ７１３）。

上記ステップＳ７０４で未通知データがない場合、または上記ステップＳ７０８もしくはＳ７１３の後、データ処理部１０３は図２３に示した画面Ｄ１６のように現在利用可能な残高を表示する（Ｓ７１４）。

続いて、携帯電話機１３の決済モードがオンになり、データ処理部１３１は図２３に示した画面Ｄ１７を表示装置１３７上に表示する（Ｓ７１５）。

続いて、利用者１２は携帯電話機１３を読取装置２７０にセットする（Ｓ７１６）。これにより、データ処理部１３１は図２３に示した画面Ｄ１８を表示装置１３７上に表示する。このとき、実在店舗のＰＯＳ端末２７においては、データ処理部２７１が読取装置２８を通じて携帯電話機１３に決済金額を送信する（Ｓ８０１）。

携帯電話機１３においては、データ処理部１３１はＰＯＳ端末２７から送信さ

れた決済金額を受信する（Ｓ７１７）。

続いて、データ処理部１３１は受信した決済金額が現在の残高内か否かを判別する（Ｓ７１８）。決済金額が残高を超えている場合、データ処理部１３１は図２３に示した画面Ｄ１９を表示装置１３７上に表示し、残高不足を利用者１２に通知する（Ｓ７１９）。

決済金額が残高内の場合、データ処理部１３１は携帯電話機１３の電話番号およびＲＯＭ１３３に予めハード的に登録されているキーコードを読取装置２８を通じてＰＯＳ端末２７に送信する（Ｓ７２０）。

ＰＯＳ端末２７においては、データ処理部２７１が携帯端末機１３から送信された携帯電話番号およびキーコードを受信する（Ｓ８０２）。

続いて、データ処理部２７１は受信した携帯電話番号およびキーコードならびに決済内容をハードディスク２７３に記録する（Ｓ８０３）。

続いて、データ処理部２７１は決済完了の情報を読取装置２７０を通じて携帯電話機１３に送信する（Ｓ８０４）。

携帯電話機１３においては、データ処理部１３１がＰＯＳ端末２７から送信された決済完了の情報を受信し、取引完了を確認する（Ｓ７２１）。

続いて、データ処理部１３１はこのときの決済金額などを含む決済内容を未通知データとしてＲＡＭ１３２に記憶する（Ｓ７２２）。

上記ステップＳ７１６～Ｓ７２２の間、データ処理部１３１は図２３に示した画面Ｄ１８を表示装置１３７上に表示する。また、携帯電話機１３が途中で読取装置２７０から取外された場合は異常終了となる。上記ステップＳ７２２で決済内容をＲＡＭ１３２に記憶した後、データ処理部１３１は図２３に示した画面Ｄ２０を表示装置１３７上に表示する。そして、上記決済モードはオフになる（Ｓ７２３）。

続いて、データ処理部１３１は電波圏内か否かを判別し（Ｓ７２４）、電波圏内の場合、ＲＡＭ１３２に蓄積されている未通知データをＲＯＭ１３３にプログラムされているキーコードとともに携帯電話会社１０のサーバ３０に送信する（Ｓ７２５）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機

１３から送信された未通知データをキーコードとともに受信する（Ｓ９０９）。

続いて、データ処理部３０１は、携帯電話機１３から送信されたキーコードを、個人情報データベース１１に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する（Ｓ９１０）。キーコードが一致しない場合、データ処理部３０１は本サービス利用不可の情報を携帯電話機１３に電波で送信する（Ｓ９１１）。携帯電話機１３は、この情報を受信し（Ｓ７２６）、続いて本サービスが利用できない旨を表示装置１３７上に表示し（Ｓ７２７）、そして本サービス手続が異常に終了した旨を表示装置１３７上に表示する（Ｓ７２８）。

上記ステップＳ９１０でキーコードが一致する場合、データ処理部３０１は受信した未通知データに基づいて利用履歴データベース２８を更新し、仮想口座１１０の前受残高を更新する（Ｓ９１２）。

続いて、データ処理部３０１は最新の前受残高を携帯電話機１３に送信する（Ｓ９１３）。

携帯電話機１３においては、携帯電話会社１０のサーバ３０から送信された前受残高を受信し、この受信した前受残高と同じになるようにＲＡＭ１３２に記憶されている前払残高を更新し、さらに未通知データをクリアする（Ｓ７２９）。

一方、実在店舗２６のＰＯＳ端末２７においては、データ処理部２７１が上記決済内容を携帯電話会社１０のサーバ３０に送信する（Ｓ８０５）。決済内容の送信は取引ごと、つまりリアルタイムで行なうのが望ましいが、営業終了後に一括してバッチ処理で行なってもよい。

携帯電話会社１０のサーバ３０においては、データ処理部３０１はＰＯＳ端末２７から送信された決済内容を受信する（Ｓ９０６）。

続いて、データ処理部３０１は決済完了の情報をＰＯＳ端末２７に送信する（Ｓ９０７）。そして、携帯電話会社１０は決済内容に基づいて実在店舗２６に対して支払処理を行なう（Ｓ９０８）。

ＰＯＳ端末２７においては、データ処理部２７１が携帯電話会社１０のサーバ３０から送信された決済完了の情報を受信する（Ｓ８０６）。

上記第１の実施の形態ではＰＯＳ端末２７から決済金額を携帯電話機１３に送信し、携帯電話機１３が決済の可否を判定しているが、携帯電話機１３から仮想

口座の残高をＰＯＳ端末２７に送信し、ＰＯＳ端末２７が決済の可否を判定するようにしてもよい。また、上記第１の実施の形態では携帯電話機１３を読取装置２７０を用いてＰＯＳ端末２７に電気的に接続しているが、近距離無線（たとえばブルートゥース(Bluetooth)）、無線ＬＡＮ(Local Area Network)またはＩｒＤＡ(Infrared Data Association)で接続したり、あるいはバーコードリーダを用いて光学的に接続してもよい。バーコードリーダを用いる場合、携帯電話機１３からＰＯＳ端末２７に送信するデータをバーコードで表示装置１３７に表示し、これをバーコードリーダで読取るようにすればよい。これらの変更は後述する実施の形態でも適用可能である。

７．本サービスの利点

７－１．クレジットカード番号、キャッシュカード番号、口座番号がインターネット上に流れない。

クレジットによる決済の場合、クレジットカード番号さえあれば決済可能な場合があり、特にインターネット上の決済においては、利用者はクレジットカード番号を入力することに強い不安と抵抗を感じることになり、事実、第三者にクレジットカード番号を知られると決済されてしまう危険性や、店頭においてもカード番号が盗まれる危険性は否定できない。しかしながら、この実施の形態ではインターネット上に流れる決済取引データにクレジットカード番号は含まれておらず、携帯電話番号がその役目を果たすものである。また、携帯電話番号はその利用目的上、広く第三者に知られているが、第三者が他人の携帯電話番号のみを知っていても携帯電話機そのものを持っていないと、実在店舗でもインターネット上の仮想店舗でも決済を完了できないうえ、決済限度額が仮想口座内の残高に限定されるため、安全性は高い。

７－２．決済の際に信用照会および承認が不要である。

利用者が携帯電話会社の仮想口座に資金を預ける（前払）する際に、その支払方法ごとに必要とされる信用照会および承認が行なわれるので、利用者がインターネット上の仮想店舗や実在店頭で決済するときには、決済金額が前払残高以内であるか否かを確認するだけでよい。現在、店頭決済時に必要とされている承認番号の取得や本人の署名などの手続が不要となる。

APPL-1002
APPLE INC. / Page 681 of 1892

７－３．店頭決済時に電波を飛ばす必要がない（電波圏外でもよい）。

この実施の形態では、店頭決済時に携帯電話機から必ずしも電波を飛ばす必要はない。したがって、店頭決済を行なう場所が電波圏内であるかどうかを意識する必要がない。よって、電波圏外の多い都市圏の地下街やビル内部、地下鉄構内、地下に設置されている自動販売機や券売機などでも決済することが可能である。携帯電話機が電波圏外にあり、決済金額が携帯電話会社に未通知状態になっていても、携帯電話機の内部メモリに未通知金額が記憶された状態で残り、次回取引発生時には未通知データが必ず送信され、仮想口座の残高が携帯電話機と携帯電話会社との間で同期がとれている状態になってから次の決済処理に入る。

７－４．２４時間仮想口座への振替が可能である。

インターネット上の仮想店舗または実在店舗での決済時に仮想口座の残高が不足しても、原則としてその場で２４時間いつでも仮想口座への資金の振替（前払）をすることが可能であるので、時間を問わず買物ができる。

７－５．決済の際に与信枠や残高を意識する必要がない。

従来、店頭でクレジットカードによる決済をする際に利用限度額を超過するため、クレジットカードによる決済を拒否されることがあり、現金の持ち合せが十分でないときには決済そのものが不可能になることもある。そのため、複数のクレジットカードを使い分けている利用者も多く、かといって利用者が各社クレジットカードごとにその限度額を認識しておくことは現実的には困難である。これに対し、この実施の形態では利用者がいつでも携帯電話会社内の仮想口座に振替済である金額、つまり前払残高を携帯電話機で確認することが可能であり、その上その残高内であれば常に決済可能であることが保証されている。

７－６．利用者は、クレジットカードやデビットカードなどの既存決済手段を提供している売り手から提供されている各サービスプログラムを継続して利用可能である。

利用者は、クレジットカードなどの既存決済手段等を利用して携帯電話会社の仮想口座に資金を振込むことで、信販会社などが提供しているサービスを継続して受けることができる。

７－７．クレジットカードを持てない世代でも後払が可能である。

APPL-1002
APPLE INC. / Page 682 of 1892

利用者が携帯電話会社内の仮想口座に「通話料に加算」という支払方法で資金の振替を指定する場合、実際に利用者の口座から資金が引落されるのは通話料金の引落し時点である。よって、クレジットカードを持てない世代でも通話料の引落し時に口座に資金があればよいことになり、クレジットカードのような「擬似翌月一括払」が可能となる。

７－８．宅配業者が提供する「代金引換え」において利用可能となれば、利用者は予め現金を準備しておく必要がなくなる。

宅配業者は、商品配達時に代金を回収する手段として、携帯電話機による決済を導入することにより、利用者は現金を予め用意する必要がなくなり、宅配業者は配達員に釣銭を持たせる必要が軽減する。店頭のＰＯＳ端末のように携帯電話会社のサーバと決済ごとにデータの送受信を行なわず、一括してその日の業務終了後に送信する方法や、その都度無線で送受信する方法等が考えられる。また、こういった移動先での決済を可能とする端末は、小規模店舗等でも流用可能であるうえ、導入が容易である。

７－９．銀行振込やコンビニエンスストアでの決済と比較して手数料が割安である。

携帯電話会社内の仮想口座への資金の振替を「通話料に加算」という支払方法で行なう場合、利用者は１００円～２００円程度の月額使用料を支払う。少額決済を同じ月内に繰返し行なう場合等は、銀行振込みやコンビニエンスストアでの決済を利用する場合よりも利用者が負担する手数料が安く済むことになる。

７－１０．手数料負担が公平である。

現行のクレジットカードやデビットカードによる決済では、手数料を加盟店が負担しており、その課金方法では少額決済では売上利益を圧迫するため、クレジットカードやデビットカードによる決済を採用していない（加盟していない）店舗がある。一方、この実施の形態では携帯電話会社への資金振込みの際にクレジットカードやデビットカードを利用する場合、極端な少額を振替える例は少ないと想定され、必要に応じて携帯電話会社が資金振替の際の最低金額やその単位を予め設定することにより、携帯電話会社が負担する信販会社等に支払う手数料と収入金額のバランスを取ることが可能である。一方、携帯電話会社から加盟店へ

APPL-1002
APPLE INC. / Page 683 of 1892

資金を振替える際には、その振替金額の一定期間中の合計に対して手数料が計算され、課金される。つまり、利用者が決済するごとに、その決済金額に対して手数料が加盟店に課金される現状のクレジットカードやデビットカードによる決済方法とは違い、加盟店は携帯電話会社からその合計金額に対する手数料を課金されることになり、少額決済の多い店舗（企業）であっても導入しやすく、個々の取引決済金額の大小にかかわらず、手数料負担が公平である。つまり、従来の決済システムでは、少額決済が大半を占める店舗、企業（たとえばコンビニエンスストア）でも、利益率を圧迫されることがない。

７－１１．少額取引に適した決済システムである。

上記７－１０のとおり、手数料負担が公平であることから、少額決済が大半を占める店舗や企業（たとえばコンビニエンスストア）でも、売上利益を圧迫されることはない。また、クレジットカードやデビットカードによる決済方法を導入している店舗や企業でも、負担する手数料の売上金額に対する割合を考慮し、利用可能な最低決済金額（たとえば３０００円以上）が設けられていることが多いが、この実施の形態では手数料は一定期間中の合計決済金額に対して課金されるので、限度額設定の必要がない。

７－１２．携帯電話機に金銭的な価値を付加するものではない。

現在、進行中の電子マネー計画では携帯電話機に金銭情報そのものをダウンロードして利用することを目的としているが、この実施の形態では仮想口座から振込を実現するための道具として携帯電話機を使用するものであり、電子マネーを仮想口座に振込む資金として利用することも可能である。商取引に携帯電話会社および決済サイトを介在させることにより、その安全性と利便性を高めることが目的であり、携帯電話機に金銭価値を付加するものではない。したがって、電子マネーは紛失したら現金を紛失することと同じであるが、この実施の形態では携帯電話機を落としても金銭的価値が消失するものではない。

７－１３．端末の不正使用に対する安全性

紛失や盗難の際も携帯電話会社にサービス停止を依頼することが可能であり、サービス停止になるまでに店頭で悪用されたとしても、利用できる金額は仮想口座内の残高内である。また、本人が携帯電話機を所有しているにもかかわらず、

APPL-1002
APPLE INC. / Page 684 of 1892

その携帯電話番号がインターネット上で第三者に悪用された場合でも、他の決済手段では決済が完了するまでまたは利用明細書が届くまで本人が認識することが困難であるのに対し、この実施の形態では決済確認がすべて携帯電話機に送信されることから、決済が完了する前に本人が認識し、未然に防ぐことが可能である。なお、携帯電話機の利用契約者が本サービスの停止を携帯電話会社に申告している場合は、インターネット上での決済の場合は携帯電話機の利用状況の確認の際に、実在店舗での決済の場合は決済モードをオンにする際にサービスの利用不可として通知される。

７－１４．携帯電話機と携帯電話会社のサーバ間での取引の安全性が高い。

携帯電話機から携帯電話会社のサーバには携帯電話番号とキーコードとがペアで送信され、携帯電話会社はこの両者を用いて認証を行なっている。携帯電話番号は利用者に固有で、キーコードは携帯電話機に固有であるから、利用者１２の携帯電話番号を知っている第三者であっても、利用者１２自身の携帯電話機１３以外の携帯電話機を使って上述した取引を行なうことはできない。

７－１５．短時間で決済が完了する。

上記７－２のとおり、与信照会は前払い時に行ない、決済時には行なう必要がないので、決済にかかる時間は短い。この時間は、現在実在店舗で行なわれているクレジットカードやデビッドカードによる決済にかかる時間よりも短い。

［第２の実施の形態］

以上、本発明の実施の形態を説明したが、本発明はその他の形態でも実施可能なものである。たとえば上記実施の形態では携帯電話会社に仮想口座を設けているが、銀行のような金融機関に仮想口座を設けてもよく、要するに携帯電話機と直接または間接的に通信可能なサーバに仮想口座を設ければよい。以下、本発明の第２の実施の形態を上記第１の実施の形態との相違点を中心に説明する。

１．資金移動

図２５は、この発明の第２の実施の形態における資金移動を示す概略図である。図１に示した第１の実施の形態と異なり、この第２の実施の形態では図２５に示すように、利用者１２の仮想口座１１０が銀行などの金融機関７０のサーバコンピュータに設けられる。この仮想口座１１０には残高の他、実在口座番号、仮想

口座番号、携帯電話会社、および携帯電話番号が記憶される。実在口座番号としては、利用者１２が金融機関７０に実際に開設している口座の番号が登録される。仮想口座番号としては、この仮想口座１１０を特定するための番号が登録される。携帯電話会社としては、利用者１２が契約している携帯電話会社１０の名称が登録される。携帯電話番号としては、利用者１２の携帯電話機１３の携帯電話番号が登録される。

金融機関７０には仮想口座１１０の他、利用者１２の実在口座７１０、仮想口座１１０の入出金履歴データベース７１２、および仮想口座１１０の決済履歴データベース７１４が設けられる。利用者１２の実在口座７１０には、実在口座番号および口座残高が記憶される。入出金履歴データベース７１２には、仮想口座１１０の口座番号と、仮想口座１１０の入出金の日付と、その入出金額とが記憶される。決済履歴データベース７１４には、仮想口座１１０の口座番号と、仮想口座１１０の入出金の日付と、決済金額と、携帯電話機１３にその時点での仮想口座残高を携帯電話機１３に通知したか否かを示す状態とが記憶される。一方、携帯電話会社１０のサーバコンピュータにおける個人情報データベース１１には利用者１２が取引している金融機関７０の名称が記憶される。

図２６は、資金移動に用いられる携帯電話機、携帯電話会社のサーバ、および金融機関のサーバのハードウェア構成を示すブロック図である。上記図７に示した第１の実施の形態と異なり、この第２の実施の形態では図２６に示すように携帯電話会社１０のサーバ３０のデータベース３０２には前受け履歴や決済履歴は記録されない。また、この個人情報データベース１１には仮想口座情報は記録されない。その代わり、金融機関７０のサーバ７２にはデータベース７０２が設けられ、このデータベース７０２に仮想口座情報１１０、仮想口座入出金履歴７１２、および仮想口座決済履歴７１４が記録される。サーバ７２のデータ処理部７０１はサーバ３０のデータ処理部３０１と通信し、データベース７０２を用いて決済処理を行なう。

図２７および図２８は、金融機関７０の仮想口座１１０に資金を振替える場合における携帯電話機１３、携帯電話会社のサーバ３０、および金融機関のサーバ７２の動作を示すフローチャートである。図２９は、この場合に携帯電話機１３

APPL-1002
APPLE INC. / Page 686 of 1892

に表示される画面の遷移図である。

図２７に示すようにこの第２の実施の形態では、ステップＳ１０４において、利用者１２は携帯電話機１３の入力装置１３６を操作して所望の振替金額を入力する。これにより、入力装置１３６はその入力された振替金額をデータ処理部１３１に与える。

続いて、携帯電話機１３の送受信部１３５は、携帯電話番号、キーコードおよび未通知データとともに、その入力された振替金額を携帯電話会社１０のサーバ３０に送信する。

携帯電話会社１０のサーバ３０においては、上記第１の実施の形態と同様に、受信した携帯電話番号およびキーコードを用いて認証を行なった後（Ｓ２０２，Ｓ２０３）、図２８に示すように利用者１２の取引銀行へ振替依頼を送信する（Ｓ２４０）。具体的には、利用者１２の個人情報データベース１１から利用者１２の取引銀行の名称（ここではＢ銀行）を読出し、Ｂ銀行のサーバ７２に利用者１２の携帯電話番号および振替金額を送信し、これにより利用者１２の実在口座７１０から仮想口座１１０にその送信した金額を振替えるよう依頼する。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された上記振替依頼を受信する（Ｓ１０００）。

続いて、データ処理部７０１は利用者１２の実在口座７１０を参照して振替が可能か否かを判定する（Ｓ１００１）。依頼のあった振替金額が実在口座７１０の残高を超えている場合、データ処理部７０１は振替不可の情報を携帯電話会社１０のサーバ３０に送信する（Ｓ１００２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された振替不可の情報を受信し（Ｓ２４１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ２４２）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された振替不可の情報を受信する（Ｓ１４０）。

続いて、データ処理部１３１は表示装置１３７上に図２９に示した画面Ｄ２１を表示し（Ｓ１４１）、残高不足のために振替ができない旨を利用者１２に通知する。

APPL-1002
APPLE INC. / Page 687 of 1892

続いて、データ処理部１３１は表示装置１３７上に異常終了を表示する（Ｓ１４２）。

上記ステップＳ１００１において依頼のあった振替金額が実在口座７１０の残高以内の場合、データ処理部７０１はその依頼のあった金額を実在口座７１０から仮想口座１１０に振替える（Ｓ１００４）。

続いて、データ処理部７０１は上記振替金額に基づいて入出金履歴データベース７１２を更新する（Ｓ１００５）。

続いて、上記ステップＳ１０００で受信した情報の中に未通知データがあるか否かをデータ処理部７０１が判別する（Ｓ１００５）。上記ステップＳ７０４で未通知データが存在し、上記ステップＳ１０６で携帯電話機１３から携帯電話会社１０に未通知データを送信し、さらに上記ステップＳ２４０で携帯電話会社１０から金融機関７０に未通知データを送信している場合、データ処理部７０１はその未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１００６）。未通知データが存在しない場合、データ処理部７０１は仮想口座１１０の残高を携帯電話会社１０に送信する（Ｓ１００７）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された仮想口座１１０の残高を受信し（Ｓ２４３）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ２０７）。

携帯電話機１３においては、上記第１の実施の形態と同様に送受信部１３５が携帯電話会社１０から送信された仮想口座１１０の残高を受信し（Ｓ１１３）、データ処理部１３１がＲＡＭ１３２に記録されている仮想口座の残高を更新し（Ｓ１１４）、最後に表示装置１３７上に振替が完了した旨を表示する（Ｓ１１５）。ここで、未通知データが存在する場合はその未通知データをクリアする（Ｓ１４３）。

２．仮想店舗での決済

図３０は、この発明の第２の実施の形態による仮想店舗での決済を示す概略図である。図３０に示すように、ここではインターネット上の仮想店舗２４と金融機関７０との間に決済機関８０が設けられる。決済機関８０は本サービスが利用される度に決済情報８１０を蓄積し、蓄積した多数の決済情報８１０に基づいて

仮想店舗２４に対して利用代金を一括して支払う。決済情報８１０には、銀行名として金融機関７０の名称、支払者名として利用者１２の氏名または名称、振替金額、仮想口座１１０の仮想口座番号、および支払先としてインターネット上の仮想店舗２４の名称が含まれている。

図３１は、仮想店舗での決済に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、金融機関７０のサーバ７２、決済機関８０のサーバ８２、および仮想店舗２４のサーバ５０のハードウェア構成を示すブロック図である。図３１に示すように、決済機関８０のサーバ８２には、データ処理部８０１と、データベース８０２とが設けられる。データベース８０２には決済情報８１０が蓄積される。データ処理部８０１はサーバ７２のデータ処理部７０１と通信し、データベース８０２に蓄積した決済情報８１０に従って仮想店舗２４に対して支払処理を行なう。

図３２～図３４は、仮想店舗２４で決済を行なう場合におけるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、仮想店舗２４のサーバ５０、および金融機関７０のサーバ７２の動作を示すフローチャートである。ここでは説明を簡単にするために、決済機関８０のサーバ８２の動作を省略する。

図１７に示した第１の実施の形態と同様に、携帯電話会社１０のサーバ３０は仮想店舗２４からの請求データを携帯電話機１３に送信する（Ｓ５０５）。

携帯電話機１３においては、送受信部１３５がその請求データを受信する（Ｓ４０１）。

続いて、その電子メールで送られてきた電子請求書を開封する（Ｓ４２０）。

続いて、上記第１の実施の形態と同様に未通知データを処理した後（Ｓ４０５～Ｓ４０７）、データ処理部１３１が表示装置１３７上に請求内容および利用可能残高（たとえば図３５に示した画面Ｄ２２またはＤ２３）を表示する（Ｓ４２１）。

続いて、データ処理部１３１は請求額が利用可能残高以内か否かを検証する（Ｓ４２２）。請求額が利用可能残高以内の場合、図３５の画面Ｄ２２のように「支払」のボタンが表示される。請求額が利用可能残高を超えている場合、図３

５の画面Ｄ２３のように「お財布にお金を入れる」のボタンが表示される。

請求額が利用可能残高を超えている場合、データ処理部１３１は利用者１２の操作に応じて追加資金を振替えるか否かを判別する（Ｓ４２３）。追加資金を振替える場合は上述した資金振替を行ない（Ｓ４２４）、追加資金を振替えない場合はステップＳ４０３に移る。

上記ステップＳ４２２で請求額が利用可能残高以内の場合、上記第１の実施の形態と同様に利用者１２が決済を承認したか否かを判別する（Ｓ４０２）。

また、携帯電話会社１０のサーバ３０において、パスワードを確認した後（Ｓ５１２）、データ処理部３０１は金融機関７０に対して決済依頼の情報を送信するとともに、未通知データが存在する場合はその未通知データを送信する（Ｓ５２０）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された決済依頼の情報を受信する（Ｓ１１００）。

続いて、データ処理部７０１は受信した決済金額を利用者１２の仮想口座１１０から振替える（Ｓ１１０１）。未通知データを受信している場合、その未通知の決済金額も利用者１２の仮想口座１１０から振替える。ここでは、仮想店舗２４への決済金額の振替を決済機関８０に依頼する。決済機関８０は依頼のたびにその決済金額を仮想店舗２４に支払うのではなく、たとえば所定の月度単位で複数の決済金額をまとめて仮想店舗２４に支払う。このような決済機関８０は必ずしも必要なく、金融機関７０が決済金額を直接仮想店舗２４に支払うようにしてもよい。ただし、決済機関８０を設けた方が振替の度に発生する手数料を抑えることができる。

続いて、データ処理部７０１はその決済金額に基づいて入出金履歴データベース７１２を更新する。（Ｓ１１０２）。

続いて、データ処理部７０１はその決済金額に基づいて決済履歴データベース７１４を更新する。（Ｓ１１０３）。

続いて、データ処理部７０１は仮想口座１１０の残高を読出して携帯電話会社１０に送信する（Ｓ１１０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７

０から送信された仮想口座残高を受信し（Ｓ５２１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ５１６）。

３．実在店舗での決済

図３６は、この発明の第２の実施の形態による実在店舗での決済を示す概略図である。図３６に示すように、実在店舗で決済する場合も決済機関８０が金融機関７０からの振替依頼を一括して実在店舗２６に対して支払を行なう。

図３７は、実在店舗での決済に設けられる携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０、金融機関７０のサーバ７２、および決済機関８０のサーバ８２のハードウェア構成を示すブロック図である。

図３７に示すように、決済機関８０のサーバ８２におけるデータ処理部８０１はサーバ７２のデータ処理部７０１と通信し、決済情報８１０に従って実在店舗２６に対する支払を行なう。

図３８～図４０は、実在店舗で決済する場合における携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０、および金融機関７０のサーバ７２の動作を示すフローチャートである。

上記図２１に示した第１の実施の形態と異なり、この第２の実施の形態では図３８に示したステップＳ７０７において、携帯電話機１３のデータ処理部１３１はＲＡＭ１３２に記録されている仮想口座残高からステップＳ７０７で計算した累計未通知金額を減算する。

また、携帯電話会社１０のサーバ３０において、ステップＳ９０２でキーコードの一致を確認した場合、データ処理部３０１は未通知データを金融機関７０のサーバ７２に送信する（Ｓ９２０）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された未通知データを受信する（Ｓ１２００）。

続いて、データ処理部７０１は受信した未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１２０１）。

続いて、データ処理部７０１は仮想口座１１０の仮想口座残高を携帯電話会社１０のサーバ３０に送信する（Ｓ１２０２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７

０から送信された仮想口座残高を受信し（Ｓ９２１）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ１０５）。

携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された仮想口座残高を受信し（Ｓ７１２）、さらにデータ処理部１３１はその受信した仮想口座残高に基づいてＲＡＭ１３２に記録されている仮想口座残高を更新しかつ未通知データをクリアする（Ｓ７１３）。

また、携帯電話会社１０のサーバ３０においては、ステップＳ９０６で実在店舗２６から送信された決済内容を受信した後、データ処理部３０１がその受信した決済内容を金融機関７０のサーバ７２に送信する（Ｓ９２２）。金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された決済内容を受信する（Ｓ１２０３）。

続いて、データ処理部７０１はその受信した決済内容に基づいて決済履歴データベース７１４を更新する（Ｓ１２０４）。

続いて、データ処理部７０１は決済完了の情報を携帯電話会社１０のサーバ３０に送信する（Ｓ１２０５）。そして、金融機関７０は上記仮想店舗の場合と同様に決済機関８０を通じて実在店舗２６に対する支払処理を行なう（Ｓ１２０６）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された決済完了の情報を受信し（Ｓ９２３）、引続きこれを実在店舗２６のＰＯＳ端末２７に送信する（Ｓ９０７）。

また、携帯電話会社１０のサーバ３０においては、ステップＳ９０９でキーコードの一致を確認した場合、データ処理部３０１はステップＳ９０９で受信した未通知データを金融機関７０のサーバ７２に送信する（Ｓ９２４）。

金融機関７０のサーバ７２においては、データ処理部７０１が携帯電話会社１０から送信された未通知データを受信しする（Ｓ１２０７）。

続いて、データ処理部７０１はその受信した未通知データに基づいて決済履歴データベース７１４を更新する（Ｓ１２０８）

続いて、データ処理部７０１は仮想口座１１０の仮想口座残高を読出して携帯電話会社１０のサーバ３０に送信する（Ｓ１２０９）。

APPL-1002
APPLE INC. / Page 692 of 1892

携帯電話会社１０のサーバ３０においては、データ処理部３０１が金融機関７０から送信された仮想口座残高を受信し（Ｓ９２５）、引続きこれを利用者１２の携帯電話機１３に送信する（Ｓ９１３）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された仮想口座残高を受信し（Ｓ７３０）、さらにその受信した仮想口座残高に基づいてＲＡＭ１３２に記録されている仮想口座残高を更新しかつ未通知データをクリアする（Ｓ７２９）。

以上のようにこの発明の第２の実施の形態によれば、仮想口座１１０を金融機関７０に設けているため、仮想口座１１０への資金移動が上記第１の実施の形態に比べて簡単になる。

上記第２の実施の形態では金融機関７０に実在口座７１０とは別に仮想口座１１０を設けているが、実在口座７１０をそのまま仮想口座１１０として取扱うようにしてもよい。この場合、実在口座７１０から仮想口座１１０への資金移動が不要となるため、処理手続はさらに簡単になる。

上記実施の形態のインターネット上の仮想店舗での決済では利用者はパーソナルコンピュータを用いて注文をしているが、携帯電話機を用いて注文をする場合もある。この場合、携帯電話機がパーソナルコンピュータの代わりの機能を果たす。

［第３の実施の形態］

仮想口座を上記第１の実施の形態では携帯電話会社に設け、上記第２の実施の形態では金融機関に設けているが、以下に述べる第３の実施の形態では携帯電話会社や金融機関とは別個の決済機関に仮想口座を設ける。

１．サービスの概要

この第３の実施の形態によるサービスの利用を希望する利用者は、仮想口座に前払金を入金するために必要な銀行の口座番号や信販会社のクレジットカード番号などを決済機関に予め登録しておく。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社を通じて決済機関に要請する。決済機関は、予め登録されている銀行の口座番号や信販会社のクレジットカード番号などを用い、利用者に対して前払金の請求を行なう。決済機関は、前

APPL-1002
APPLE INC. / Page 693 of 1892

払金の請求後、前払金を仮想口座に入金した上で仮想口座の残高を携帯電話会社を介して携帯電話機に送信する。仮想店舗や実在店舗は、上記第１および第２の実施の形態のように携帯電話会社や金融機関ではなく、決済機関に対して請求を行なう。

１－１．利用登録

図４１は、携帯電話機１３の利用者１２が本サービスの利用を希望する場合に最初に行なう利用登録の方法を示す概略図である。図４１に示すように、本サービスの利用を希望する利用者１２は、加入している携帯電話会社、携帯電話番号、および前払金を引落すための銀行の口座番号や信販会社のクレジットカード番号といった決済情報を所定の引落口座登録用紙２５に記入して決済機関９０に郵送する。決済機関９０は、引落口座登録用紙２５に基づいて利用者情報９１０をデータベースに登録する。

続いて、決済機関９０は、利用者１２に付与した会員番号（利用者情報９１０中の顧客番号）を携帯電話会社１０を通じて利用者１２に通知する。利用者１２はその通知内容を確認し、問題がなければ携帯電話会社１０を通じて決済機関９０に対して本サービスの申込を承認する。これに応じて決済機関９０は、仮想口座１１０を開設するとともに、仮想口座の入出金履歴９１２や決済履歴９１４を記録するための領域をデータベース内に開設する。

なお、決済機関９０のデータベースには、本サービスの利用が可能な加盟店（仮想店舗および実在店舗を含む）とその加盟店における利用金額を振込むための振込口座などの加盟店情報９１６が登録されている。

続いて、決済機関９０は、本サービスの開始を携帯電話会社１０を通じて利用者１２の携帯電話機１３に通知する。このとき、携帯電話会社１０は個人情報１１の利用状況を「未登録」から「利用可」に変更する。利用者１２の携帯電話機１３が携帯電話会社１０から本サービス開始の通知を受けると、携帯電話機１３の利用状況を「利用不可」から「利用可」に変更する。

上記手続により、利用者１２は本サービスの利用が可能となる。

１－２．仮想口座への資金移動

図４２は、決済機関９０に設けた仮想口座１１０に入金する前払金を金融機関

APPL-1002
APPLE INC. / Page 694 of 1892

の口座から引落しする場合の資金移動を示す概略図である。図４２に示すように、利用者１２は携帯電話機１３を用い、携帯電話会社１０を通じて決済機関９０に対して所望の前払金を仮想口座１１０に入金するよう要請する。ここでは仮想口座１１０に５０００円を入金する場合を例示している。決済機関９０は仮想口座１１０への前払の要請を受けると、利用者情報９１０に基づき、利用者１２の口座１６０が開設されている銀行や信販会社のような金融機関１７０に対して前払金の引落しを依頼する。引落し依頼を受けた金融機関１７０は引落しが可能か否かを確認し、可能な場合は振替データを決済機関９０に送り、前払金を決済機関９０に支払う。引落しが不可能な場合はその旨決済機関９０に通知する。決済機関９０は金融機関１７０から振替データを受けると、入出金履歴９１２を更新し、さらに仮想口座１１０を更新する。続いて、決済機関９０はその更新した仮想口座１１０の残高を携帯電話会社１０に通知する。携帯電話会社１０では、携帯電話番号や仮想口座残高などの送信データ１０２が作成される。携帯電話会社１０はこの送信データ１０２に基づいて利用者１２に仮想口座残高を通知する。この通知に応じて利用者１２の携帯電話機１３は仮想口座残高を更新する。携帯電話会社１０から利用者１２の携帯電話機１３への送信データ１０２の送信が完了すると、送信データ１０２はクリアされる。利用者１２が電波圏外にいる場合など、送信データ１０２の送信が不可能な場合、送信データ１０２はクリアされずにそのまま保持される。

１－３．仮想店舗での決済

図４３は、携帯電話機１３を用いてインターネット上の仮想店舗２４で決済する方法を示す概略図である。図４３に示すように、利用者１２は携帯電話機１３またはパーソナルコンピュータ４０を用いて仮想店舗２４に対して注文を出す。注文を受けた仮想店舗２４は、利用者１２の顧客番号や請求内容などを記載した電子請求書を決済機関９０および携帯電話会社１０を通じて利用者１２の携帯電話機１３に送信する。利用者１２はその送信された電子請求書を携帯電話機１３で確認し、その請求内容が自らの注文内容と一致する場合は決済の承認を携帯電話会社１０を通じて決済機関９０に通知する。決済機関９０は決済の承認を得ると、その請求内容に応じて入出金履歴９１２および決済履歴９１４を更新すると

ともに、仮想口座１１０の残高も更新する。ここではＢ店という仮想店舗２４で３０００円の商品を購入した場合を例示している。

続いて、決済機関９０はその更新した仮想口座残高を携帯電話会社１０に通知する。携帯電話会社１０はその仮想口座残高を送信データ１０２とし、さらに利用者１２の携帯電話機１３に送信する。これに応じて携帯電話機１３の仮想口座残高が更新される。携帯電話会社１０から利用者１２への仮想口座残高の送信が完了すると、送信データ１０２はクリアされる。

一方、決済機関９０は仮想口座残高の更新を終えると、決済の完了を仮想店舗２４を通じて利用者１２に通知する。また、決済機関９０は加盟店情報９１６に基づいてその決済金額を加盟店の振込口座に入金する。

１－４．実在店舗での決済

図４４は、携帯電話機１３を用いて実在店舗２６で決済する方法を示す概略図である。図４４に示すように、実在店舗２６に設置されているＰＯＳ端末２７に携帯電話機１３が装着されると、ＰＯＳ端末２７は決済金額を携帯電話機１３に送信する。決済金額が仮想口座残高以内の場合、携帯電話機１３は決済内容を未通知データに記録するとともに、携帯電話番号、キーコードおよびパスワードをＰＯＳ端末２７に送信する。これに応じて、ＰＯＳ端末２７は決済の完了を携帯電話機１３に通知する。

その後、ＰＯＳ端末２７は、携帯電話番号、キーコードおよびパスワードとともに決済内容を決済機関９０に通知する。決済機関９０は、受信した携帯電話番号、キーコードおよびパスワードを携帯電話会社１０に送信することにより認証を依頼する。認証依頼を受けた携帯電話会社１０は、個人情報１１の未通知を「無」から「有」に変更する。受信した携帯電話番号、キーコードおよびパスワードが個人情報１１として登録されている携帯電話番号、キーコードおよびパスワードと一致しない場合、携帯電話会社１０は個人情報１１の利用状況を「認証異常」に変更し、その旨を利用者１２および決済機関９０に通知する。この通知に応じて、携帯電話機１３は利用状況を「認証異常」に変更する。

一方、受信した携帯電話番号、キーコードおよびパスワードが個人情報１１として登録されている携帯電話番号、キーコードおよびパスワードと一致した場合、

携帯電話会社１０は認証が正常に完了した旨を決済機関９０に通知する。この通知に応じて、決済機関９０は入出金履歴９１２および決済履歴９１４を更新する。決済機関９０はさらに、仮想口座１１０の残高を更新するとともに、未通知を「無」から「有」に変更する。ここでは、Ｄ店という実在店舗２６で１０００円の商品を購入した場合を例示している。

続いて、決済機関９０は決済が完了した旨を実在店舗２６に通知する。また、決済機関９０は加盟店情報９１６に基づいて加盟店の振込口座にその決済金額を入金する。

１－５．未通知データの要求

図４５は、利用者１２が実在店舗２６で決済をしたために携帯電話機１３内に未通知データが発生して携帯電話機１３の仮想口座残高が決済機関９０の仮想口座残高と一致しなくなった場合に決済機関９０が仮想口座残高の同期をとるために携帯電話機１３に対して未通知データの送信を要求する方法を示す概略図である。図４５に示すように、決済機関９０は携帯電話会社１０を通じて利用者１２の携帯電話機１３に未通知データを要求する。これに応じて、携帯電話機１３は携帯電話会社１０を通じて未通知データを決済機関９０に送信する。決済機関９０は、受信した未通知データに基づいて決済履歴９１４のうち該当の決済の状態を「未通知」から「通知済」に変更する。

続いて、決済機関９０は仮想口座１１０の残高を携帯電話会社１０に送信する。携帯電話会社１０は受信した仮想口座残高を送信データ１０２とするとともに、個人情報１１中の未通知を「有」から「無」に変更する。携帯電話会社１０は仮想口座残高を携帯電話機１３に送信する。これに応じて、携帯電話機１３は仮想口座残高を更新するとともに、未通知データをクリアする。携帯電話会社１０は仮想口座残高の送信を完了すると、送信データ１０２をクリアする。

１－６．請求代行

図４６は、仮想店舗２４に代わって決済機関９０が利用者１２による仮想店舗２４での決済金額を信販会社２０に請求する方法を示す概略図である。この請求代行は、決済機関９０に設けた仮想口座１１０を利用するものではなく、利用者情報９１０として登録されている銀行の口座番号や信販会社のクレジットカード

APPL-1002
APPLE INC. / Page 697 of 1892

番号を利用してデビット決済やカード決済を行なうものである。

図４６に示すように、利用者１２が携帯電話機１３またはパーソナルコンピュータ４０を用いて仮想店舗２４に対して注文をすると、仮想店舗２４は顧客番号や請求内容などからなる電子請求書を決済機関９０および携帯電話会社１０を通じて利用者１２に発行する。利用者１２は携帯電話機１３に送信された電子請求書を確認し、決済を承認する場合はその旨を携帯電話会社１０を通じて決済機関９０に通知する。その際に、予め登録している決済方法の中から１つを選択する。ここでは、信販会社Ｅ社のクレジットカードによる決済を選択した場合を例示している。

決済機関９０は決済の承認を仮想店舗２４に通知するとともに、利用者情報９１０を用いてクレジットカード番号や決済金額などの決済内容を信販会社２０に通知する。これに応じて信販会社２０は仮想店舗２４に対して決済金額の支払処理を行ない、決済が完了した旨を仮想店舗２４に通知する。

利用者１２が決済方法としてデビットカードによる決済を選択した場合、決済機関９０は利用者情報９１０を用いて口座番号や決済金額などの決済内容を銀行１７に通知する。銀行１７はその決済金額を利用者１２の口座から引落し、さらに仮想店舗２４に対してその決済金額の支払処理を行なう。

上記請求代行サービスでは、銀行の口座番号や信販会社のクレジットカード番号といった重要な決済情報は予め決済機関９０に登録されており、携帯電話機１３やパーソナルコンピュータ４０から送信されることはない。認証は携帯電話番号、キーコードおよびパスワードを用いて携帯電話会社１０で行なわれ、認証が得られた場合だけ予め登録されている口座番号やクレジットカード番号が決済機関９０から金融機関１７０や信販会社２０に通知される。したがって、高い安全性を確保することができる。

２．システム構成およびその動作

次に、上記サービスを実現するためのシステム構成およびその動作について説明する。

２－１．利用登録

図４７は、図４１に示した利用登録のためのハードウェア構成を示すブロック

APPL-1002
APPLE INC. / Page 698 of 1892

図である。上記第１および第２の実施の形態と異なり、この第３の実施の形態では、携帯電話会社１０のサーバ３０には、送信データ１０２を記憶するためのメモリ３０３が設けられる。また、決済機関９０のサーバ９２には、データ処理部９２１と、データベース９２２とが設けられる。データベース９２２には、利用者情報９１０、仮想口座の入出金履歴９１２、仮想口座の決済履歴９１４および加盟店情報９１６が蓄積される。データ処理部９２１は、携帯電話会社１０に設置されているサーバ３０のデータ処理部３０１と接続され、データベース９２２に対して所定のデータ処理を行なう。

図４８は、利用登録を行なう場合における利用者１２の携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

まず、利用者１２は携帯電話機１３の入力装置１３６を操作して本サービスの利用申込を携帯電話機１３から携帯電話会社１０に送信する（Ｓ１１）。携帯電話会社１０のサーバ３０においては、データ処理部 301 が携帯電話機１３から送信された利用申込を受信し（Ｓ２１）、これを決済機関９０に送信する（Ｓ２２）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された利用申込を受信する（Ｓ１３０１）。これに応じて、決済会社９２は所定の申込用紙を利用者１２に発送する（Ｓ１３０２）。利用者１２は申込用紙に引落しを希望する銀行の口座番号や信販会社のクレジットカード番号などを記入した後、決済機関９０に返送する。決済機関９０は利用者１２から返送された申込用紙を受取る（Ｓ１３０２）。この申込用紙に記入された事項に基づいて、データ処理部３０１は利用者情報９１０をデータベース９２２に登録する（Ｓ１３０３）。具体的には、利用者１２の会員番号、携帯電話番号、携帯電話会社、銀行の口座番号、信販会社のクレジットカード番号などを登録する。続いて、データ処理部９２１は会員番号を携帯電話会社１０に通知する（Ｓ１３０４）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された会員番号を受信し（Ｓ２３）、これを利用者１２に通知する（Ｓ２４）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電

話会社１０から送信された会員番号を受信し（Ｓ１２）、利用者１２がその申込を承認した場合はその旨を携帯電話会社１０に通知する（Ｓ１３）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された申込承認の通知を受信し（Ｓ２５）、これを決済機関９０に通知する（Ｓ２６）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された申込承認の通知を受信し(Ｓ１３０５）、仮想口座１１０を開設し（Ｓ１３０６）、本サービスの開始を携帯電話会社１０に通知する（Ｓ１３０７）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信されたサービス開始の通知を受信し（Ｓ２７）、個人情報１１の利用状況を「未登録」から「利用可」に更新する（Ｓ２８）。続いて、データ処理部３０１は本サービスの開始を利用者１２に通知する（Ｓ２９）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信されたサービス開始の通知を受信し（Ｓ１４）、利用状況を「利用不可」から「利用可」に更新する（Ｓ１５）。

２－２．仮想口座への資金移動

図４９は、図４２に示した資金移動に用いられる利用者１２の携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、金融機関１７０のサーバ１７２のハードウェア構成を示すブロック図である。図４９に示すように、金融機関１７０に設置されるサーバ１７２は、データ処理部１７４と、データベース１７６とを備える。データ処理部１７４はデータベース１７６のデータを処理するとともに、携帯電話会社１０に設置されているサーバ３０のデータ処理部３０１に接続される。データベース１７６には、利用者の住所や氏名などの利用者情報１７７と、金融機関１７０に開設されている実在口座に関する実在口座情報１７８と、実在口座における入出金などの実在口座履歴１７９とが登録される。

図５０～図５２は、図４２に示したように金融機関１７０から決済機関９０の仮想口座１１０に資金を移動する場合における携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

APPL-1002
APPLE INC. / Page 700 of 1892

ここでは、パスワードの入力（Ｓ１０１）前に、携帯電話機１３が利用状況を確認し、利用不可の場合はその旨を表示装置１３７に表示する（Ｓ１００）。利用可の場合は利用者１２に対してパスワードの入力を促す（Ｓ１０１）。また、パスワードの検証（Ｓ１０２）後、前払金額の入力（Ｓ１０４）前に、図２１と同様に未通知データを確認して利用可能残高を表示する（Ｓ７１４）。

続いて、携帯電話機１３の送受信部１３５はステップＳ１０４で入力された前払金額などを携帯電話会社１０に送信するが（Ｓ１０６）、ここではステップＳ１０１で入力されたパスワードも携帯電話会社１０に送信する。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が受信した携帯電話番号に基づいて個人情報１１を検索した後（Ｓ２０２）、受信したキーコードおよびパスワードを検証する（Ｓ２０３）。キーコードまたはパスワードが一致しない場合、個人情報１１の利用状況を「利用可」から「利用不可」に変更し（Ｓ２５０）、認証の異常を利用者１２に通知する（Ｓ２５１）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から認証異常の通知を受信し（Ｓ１５０）、これに応じてデータ処理部１３１は携帯電話機１３の利用状況を「利用可」から「認証異常」に変更し（Ｓ１５１）、本サービスの利用停止を表示装置１３７に表示する（Ｓ１５２）。

一方、ステップＳ２０３でキーコードおよびパスワードの両方が一致した場合、データ処理部３０１は個人情報１１の利用状況を確認し（Ｓ２０４）、利用状況が「利用可」の場合は未通知データがあるか否かを判定する（Ｓ２５３）。未通知データがある場合、データ処理部３０１はステップＳ２０１で受信した前払金額とともに未通知データを決済機関９０に送信する（Ｓ２５４）。一方、未通知データがない場合、データ処理部３０１は前払金額のみを決済機関９０に送信する（Ｓ２５５）。このように携帯電話会社１０から決済機関９０に前払金額を送信する際には、利用者１２の携帯電話番号も送信する。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された携帯電話番号や前払金額などを受信し（Ｓ１３００）、その受信した情報およびデータベース９２２に登録されている利用者情報９１０に基づいて利用者１２が口座を開設している金融機関１７０に対する請求データを作成

APPL-1002
APPLE INC. / Page 701 of 1892

する（Ｓ１３０１）。決済機関９０はその請求データに従って金融機関１７０に前払金額の引落しを依頼する（Ｓ１３０２）。

金融機関１７０は、決済機関９０からの引落し依頼に応じて利用者１２の口座１６０から前払金額を引落す（Ｓ１４００）。続いて、データ処理部１７４は引落しが可能か否か、すなわち前払金額が口座残高以内か否かを判定する（Ｓ１４０１）。引落しが不可能な場合、データ処理部１７４は決済機関９０にその旨を通知する（Ｓ１４０２）。決済機関９０のサーバ９２においては、データ処理部９２１が金融機関１７０から引落し不可の通知を受信し（Ｓ１３０３）、これを利用者１２の携帯電話番号とともに携帯電話会社１０に通知する（Ｓ１３０４）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から引落し不可の通知を受信し（Ｓ２５６）、これを利用者１２の携帯電話機１３に通知する（Ｓ２３２）。

一方、ステップＳ１４０１において引落しが可能な場合、サーバ１７２のデータ処理部１７４は振替データを決済機関９０に送信し（Ｓ１４０３）、利用者１２の口座１６０から決済機関９０の口座に前払金額を振替える支払処理を実行する（Ｓ１４０４）。

決済機関９０のサーバ９２においては、データ処理部９２１が金融機関１７０から送信された振替データを受信し（Ｓ１３０５）、続いて前払金額の入金をデータベース９２２に記録することにより入出金履歴９１２を更新する（Ｓ１３０６）。未通知データが送信されて来ている場合は、ここで決済金額をデータベース９２２に記録することにより決済履歴９１４を更新する（Ｓ１３０７）。続いて、データ処理部９２１は仮想口座１１０の残高に前払金額を加算することにより仮想口座残高を更新する（Ｓ１３０８）。未通知データがあった場合はこれを「無」に変更する。続いて、データ処理部９２１は仮想口座１１０の残高を携帯電話番号とともに携帯電話会社１０に送信する（Ｓ１３０９）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された仮想口座残高を受信し（Ｓ２５７）、その仮想口座残高を送信データ１０２としてメモリ３０３に記憶する（Ｓ２５８）。続いて、データ処理部３０１は未通知データを「無」に変更する（Ｓ２５９）。続いて、データ処理

APPL-1002
APPLE INC. / Page 702 of 1892

部３０１は、メモリ３０３に記憶された送信データ１０２を利用者１２の携帯電話機１３に送信する（Ｓ２６０）。続いて、上記送信が正常に終了したか否かを判定し（Ｓ２６１）、正常に終了した場合は送信データ１０２をクリアし（Ｓ２６２）、利用者１２が電波圏外にいたり携帯電話機１３の電源を切っていた場合など、送信データを携帯電話機１３に送信できず、送信が正常に終了しなかった場合は再送信処理を行なう（Ｓ２６３）。具体的には、所定期間経過後に送信データ１０２を再び携帯電話機１３に送信する。

２－３．仮想店舗での決済

図５３は、図４３に示した仮想店舗２４での決済に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２および仮想店舗２４のサーバ５０のハードウェア構成を示すブロック図である。図５３に示すように、決済機関９０に設置されたサーバ９２のデータ処理部９２１はインターネット６０に接続される。

図５４～図５６は、図４３に示したように仮想店舗２４で決済する場合におけるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、および仮想店舗２４のサーバ５０の動作を示すフローチャートである。

ここでは、利用者１２のパーソナルコンピュータ４０または携帯電話機１３は注文内容とともに会員番号（顧客番号）を仮想店舗２４に送信する（Ｓ３０１）。仮想店舗２４のサーバはこれらを受信し（Ｓ６０１）、電子請求書を作成して会員番号とともに請求内容をインターネット６０を介して決済機関９０に送信する（Ｓ６０２）。

決済機関９０のサーバ９２においては、データ処理部９２１が仮想店舗２４から送信された電子請求書を受信し（Ｓ１３１０）、その受信した会員番号に基づいてデータベース９２２を検索して利用者情報９１０の中から利用者１２の携帯電話番号および携帯電話会社を特定する（Ｓ１３１１）。続いて、データ処理部９２１は受信した電子請求書を該当の携帯電話会社１０に携帯電話番号とともに送信する（Ｓ１３１２）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９

APPL-1002
APPLE INC. / Page 703 of 1892

０から送信された電子請求書を携帯電話番号とともに受信する（Ｓ５０１）。データ処理部３０１は個人情報１１中の利用状況を確認し（Ｓ５０３）、利用状況が「利用不可」の場合はその旨を携帯電話番号とともに決済機関９０に通知する（Ｓ５０４）。

決済機関９０のサーバ９２においては、携帯電話会社１０から携帯電話番号とともに通知されたサービス利用不可の通知を受信し（Ｓ１３１３）、これをインターネット６０を介して仮想店舗２４に通知する（Ｓ１３１４）。

また、利用者１２は、携帯電話会社１０から送信され、携帯電話機１３で受信した電子請求書を開封し（Ｓ４１８）、携帯電話機１３のデータ処理部１３１は受信した電子請求書の請求内容および利用可能な仮想口座残高を表示装置１３７に表示する（Ｓ１５４）。

また、電子請求書の請求金額が利用可能残高を超えている場合、データ処理部１３１は表示装置１３７を通じて利用者１２に対して仮想口座１１０への追加振替を行なうか否かを問合せる（Ｓ１５５）。追加振替を行なう場合、データ処理部１３１は資金振替の処理を実行する（Ｓ１５６）。

また、決済を承認するか否かの判定（Ｓ４０２）は、利用可能残高の検証（Ｓ４０８）後に行なう。携帯電話会社１０のサーバ３０においては、データ処理部３０１が受信した決済の取消または拒否を携帯電話番号とともに決済機関９０に送信する（Ｓ５０７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された決済の取消または拒否を受信し（Ｓ１３１５）、これをインターネット６０を介して仮想店舗２４に送信する（Ｓ１３１６）。決済の取消または拒否は上記実施の形態と同様に仮想店舗２４を介して利用者１２に返信される（Ｓ６０５，Ｓ６０６，Ｓ３０４）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、データ処理部４０１または１３１がその受信した決済の取消または拒否（受注取消）を表示装置４０６または１３７に表示する（Ｓ３０８）。

また、利用者１２の携帯電話機１３においては、パスワードの入力（Ｓ４１１）後に、データ処理部１３１がその入力されたパスワードの検証を行なう（Ｓ１５７）。パスワードが誤っている場合はデータ処理部１３１はその旨を表示装

APPL-1002
APPLE INC. / Page 704 of 1892

置１３７に表示し（Ｓ１５８）、パスワードが正しい場合は送受信部１３５は決済の承認を携帯電話会社１０に通知する（Ｓ４１２）。

また、携帯電話会社１０のサーバ３０においては、キーコードまたはパスワードが不一致の場合、データ処理部３０１は個人情報１１の利用状況を「利用可」から「認証異常」に変更し（Ｓ５２２）、その旨を利用者１２に通知し（Ｓ５２３）、さらに決済機関９０にも携帯電話番号とともに通知する（Ｓ５２４）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された認証異常の通知を受信し（Ｓ１５９）、データ処理部１３１は利用状況を「利用可」から「認証異常」に変更し、さらに本サービスの利用停止を表示装置１３７に表示する（Ｓ１６１）。一方、決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された認証異常の通知を受信し（Ｓ１３１７）、認証異常を理由に決済が不可能である旨をインターネット６０を介して仮想店舗２４に通知する（Ｓ１３１８）。仮想店舗２４のサーバ５０においては、モデム５０４が決済機関９０から送信された決済不可の通知を受信し（Ｓ６１３）、これに応じて受注の取消をインターネット６０を介して利用者１２のパーソナルコンピュータ４０または携帯電話機１３に送信する（Ｓ６１４）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、モデム４０４または送受信部１３５が仮想店舗２４から送信された受注の取消を受信し（Ｓ３０９）、データ処理部４０１または１３１がその旨を表示装置４０６または１３７に表示する（Ｓ３１０）。

ステップＳ５１１，Ｓ５１２においてキーコードおよびパスワードがともに一致した場合、データ処理部３０１は未通知が「有」か否かを判定し（Ｓ５２５）、未通知データがある場合は決済データおよび未通知データを携帯電話番号とともに決済機関９０に送信する（Ｓ５２６）。未通知データがない場合はデータ処理部３０１は決済データを携帯電話番号とともに決済機関９０に送信する（Ｓ５２７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された決済データ（および未通知データがある場合は未通知データ）を受信し（Ｓ１３１９）、その受信した決済データ（および未通知データがある場合は未通知データ）に基づいて入出金履歴９１２を更新し（Ｓ１３２０）、

APPL-1002
APPLE INC. / Page 705 of 1892

決済履歴９１４を更新し（Ｓ１３２１）、さらに仮想口座１１０の残高を更新する（Ｓ１３２２）。ここで、データ処理部９２１は仮想口座１１０の未通知を「無」にする。

続いて、データ処理部９２１は更新した仮想口座１１０の残高を携帯電話番号とともに携帯電話会社１０に送信し（Ｓ１３２３）、決済の完了をインターネット６０を介して仮想店舗２４に通知し（Ｓ１３２４）、さらに仮想店舗２４への支払処理を行なう（Ｓ１３２５）。決済完了の通知は仮想店舗２４を介して利用者１２にも通知される（Ｓ６１２，Ｓ３０７）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、データ処理部４０１または１３１がその受信した決済の完了を表示装置４０６または１３７に表示する（Ｓ３１１）。

一方、携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０から送信された仮想口座残高を受信し（Ｓ５２８）、その残高を送信データ１０２としてメモリ３０３に記憶する（Ｓ５２９）。続いて、データ処理部３０１は個人情報１１の未通知を「無」にし（Ｓ５３０）、メモリ３０３に記憶された送信データ（仮想口座残高）１０２を利用者１２の携帯電話機１３に送信する（Ｓ５３１）。

続いて、データ処理部３０１は上記データの送信が正常に終了したか否かを判定し（Ｓ５３２）、正常に終了した場合はメモリ３０３に記憶された送信データ１０２をクリアし（Ｓ５３３）、正常に終了しなかった場合は再び送信処理を行なう（Ｓ５３４）。

利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された送信データ１０２を受信し（Ｓ１６２）、データ処理部１３１がその受信した送信データ１０２に基づいて仮想口座残高を更新する（Ｓ１６３）。続いて、データ処理部１３１は未通知データをクリアし（Ｓ１６４）、仮想口座残高とともに決済の完了を表示装置１３７に表示する（Ｓ１６５）。

２－４．実在店舗での決済

図５７は、図４４に示した実在店舗での決済に用いられる携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２

APPL-1002
APPLE INC. / Page 706 of 1892

のハードウェア構成を示すブロック図である。ここでは図２０と異なり、決済機関９０のサーバ９２が実在店舗２６のＰＯＳ端末２７および携帯電話会社１０のサーバ３０に接続される。

図５８～図６０は、図５７に示した携帯電話機１３、ＰＯＳ端末２７、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。

ここでは、携帯電話会社１０のサーバ３０において、ステップＳ５２５の判定の結果、未通知データがある場合、データ処理部３０１はその未通知データを携帯電話番号とともに決済機関９０に送信する（Ｓ５３５）。決済機関９０のサーバ９２においては、未通知データがある場合、データ処理部９２１は入出金履歴９１２を更新する（Ｓ１３３０）。続いて、データ処理部９２１は決済履歴９１４を更新し、該当する決済の状態を「通知済」とする（Ｓ１３３１）。続いて、データ処理部９２１は未通知データがある場合に仮想口座１１０の残高を更新し、未通知を「無」にする（Ｓ１３３２）。

また、ここでは図２２と異なり、利用者１２の携帯電話機１３において、残高の検証（Ｓ７１８）後に、データ処理部１３１は未通知データに決済内容を記憶し（Ｓ７２２）、その後、携帯電話番号、キーコード、パスワードといった携帯電話機１３の端末情報をＰＯＳ端末２７に送信する（Ｓ７２０）。ステップＳ８０２～Ｓ８０４，Ｓ７２１は図２２と同じである。ステップＳ７２１でＰＯＳ端末２７から決済完了の通知を受信した後、データ処理部１３１は決済モードをオフにし（Ｓ７２３）、決済の終了を表示装置１３７に表示する（Ｓ７３１）。

また、ＰＯＳ端末２７のデータ処理部２７１はステップＳ８０２で受信した携帯電話番号、キーコードおよびパスワードとともに、ステップＳ８０３で記録した決済内容を決済機関９０に送信する（Ｓ８０５）。決済機関９０のサーバ９２においては、データ処理部９２１がＰＯＳ端末２７から携帯電話番号などとともに送信された決済内容を受信し（Ｓ１３３３）、その受信した携帯電話番号に基づいてデータベース９２２に記憶された利用者情報９１０を検索する（Ｓ１３３４）。この検索結果に従って、データ処理部９２１は該当の携帯電話会社１０に認証を依頼するためにステップＳ１３３３で受信した携帯電話番号、キーコード

およびパスワードを携帯電話会社１０に送信する（Ｓ１３３５）。

携帯電話会社１０のサーバ３０においては、図５５と同様にデータ処理部３０１が認証を行なう（Ｓ５１１，Ｓ５１２）。ただしここでは、キーコードまたはパスワードが不一致の場合、データ処理部３０１は個人情報１の利用状況を「利用不可」に変更し（Ｓ５２２）、本サービスの利用停止を利用者１２に通知する（Ｓ５２３）。利用者１２の携帯電話機１３においては、データ処理部１３１は利用状況を「利用不可」に変更する（Ｓ１６０）。

一方、キーコードおよびパスワードが一致した場合、データ処理部３０１は個人情報１１の未通知を「有」に変更し（Ｓ９２５）、認証の成功を決済機関９０に通知し、さらに後述する未通知データの要求処理を行なう（Ｓ９２７）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話会社１０から送信された認証成功の通知を受信し（Ｓ１３３０）、入出金履歴９１２、決済履歴９１４および仮想口座１１０の残高をそれぞれ更新する（Ｓ１３２０～Ｓ１３２２）。ここでは、決済履歴９１４を更新したときその状態を「未通知」とする。続いて、データ処理部９２１は仮想口座１１０の未通知を「有」に変更する（Ｓ１３３１）。

また、データ処理部９２１が携帯電話会社１０から認証異常の通知を受信した場合も（Ｓ１３１７）、データ処理部９２１は実在店舗２６に対する決済金額の支払処理を行なう（Ｓ１３３２）。このような認証異常が起こる原因として利用者１２の不正が考えられるが、この場合も決済機関９０は実在店舗２６に対して支払を保証することになる。決済機関９０は不正使用による損害を負担することになるが、上記のように認証異常を検出した時点で本サービスの利用を停止しているので損害を最小限に抑えることができる。

２－５．未通知データの要求

図６１は、携帯電話会社１０が利用者１２に対して未通知データを要求する場合における携帯電話機１３、携帯電話会社１０のサーバ３０および決済機関９０のサーバ９２の動作を示すフローチャートである。なお、未通知データは図２４に示した第１の実施の形態と同様に携帯電話機１３のＲＡＭ１３２に記憶されている。また、未通知データの要求の際には図４７に示したハードウェア構成が用

いられる。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が予め定められた時間間隔おきに利用者１２の携帯電話機１３に対して未通知データの送信を要求する（Ｓ５４０）。利用者１２の携帯電話機１３においては、送受信部１３５が携帯電話会社１０から送信された未通知データの送信要求を受信し（Ｓ１７０）、これに応じてデータ処理部１３１がＲＡＭ１３２に記憶されている未通知データを携帯電話番号、キーコードおよびパスワードとともに携帯電話会社１０に送信する（Ｓ７０６）。以下、図５８および図５９と同様に携帯電話会社１０のサーバ３０は認証などを行ない、決済機関９０のサーバ９２は決済履歴９１４の更新などを行なう。

２－６．請求代行

図６２は、図４６に示した請求代行に用いられるパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、仮想店舗２４のサーバ５０、決済機関９０のサーバ９２、金融機関１７０のサーバ９４のハードウェア構成を示すブロック図である。図６２に示すように、金融機関のサーバ９４は、データ処理部９４１と、データベース９４２とを備える。データ処理部９４１は、インターネット６０と、決済機関９０に設置されているサーバ９２のデータ処理部９２１とに接続される。データベース９４２には、利用者情報９４３、加盟店情報９４４および利用者履歴９４５が蓄積される。利用者情報９４３は、利用者の住所、氏名、電話番号などの他、銀行の場合は口座番号、信販会社の場合はクレジットカード番号および引落銀行口座などである。加盟店情報９４４は、デビットカードやクレジットカードによる決済を受付ける加盟店の住所、名称などである。利用者履歴９４５は、デビットカードやクレジットカードによる決済金額、決済日、利用加盟店の名称などである。

図６３および図６４は、図６２に示したパーソナルコンピュータ４０、携帯電話機１３、携帯電話会社１０のサーバ３０、決済機関９０のサーバ９２、金融機関のサーバ９４および仮想店舗２４のサーバ５０の動作を示すフローチャートである。

図６３および図６４に示した請求代行の処理は、図５４～図５６に示した仮想

店舗での決済の処理に類似している。ただし、請求代行の際には利用者１２の携帯電話機１３において、ステップＳ４１８で電子請求書を開封した後直ちに、決済の承認を行なう（Ｓ４０２）。また、ステップＳ１５７でパスワードが一致した場合に、デビットカードによる決済かクレジットカードによる決済かという決済方法の選択を利用者１２に対して促す（Ｓ１７１）。続いて、携帯電話機１３の送受信部１３５は、決済の承認を携帯電話会社１０に通知する（Ｓ４１２）。このとき、携帯電話番号、キーコード、パスワード、決済内容の他、決済方法も合わせて携帯電話会社１０に送信する。

また、携帯電話会社１０のサーバ３０においては、ステップＳ５１１，Ｓ５１２でキーコードおよびパスワードが一致した場合に、データ処理部３０１はステップＳ５１０で受信した決済の承認を携帯電話番号とともに決済機関９０に送信する。決済機関９０のサーバ９２においては、データ処理部９２１がこの決済の承認をインターネット６０を介して仮想店舗２４に通知し（Ｓ１３３５）、仮想店舗２４のサーバ５０においてはモデム５０４がこの通知を受信する（Ｓ６１５）。

続いて、データ処理部９２１は金融機関に決済内容を通知する（Ｓ１３３６）。金融機関のサーバ９４においては、データ処理部９４１が決済機関９０から送信された決済内容を受信し（Ｓ１５００）、所定の決済処理を行なう（Ｓ１５０１）。続いて、データ処理部９４１は決済の可否を仮想店舗２４に通知する（Ｓ１５０２）。仮想店舗２４のサーバ５０においては、モデム５０４が金融機関から送信された決済可否の通知を受信し（Ｓ６１６）、決済が可能か否かを判定し（Ｓ６１７）、決済が不可能な場合は受注の取消を利用者１２のパーソナルコンピュータ４０または携帯電話機１３に送信する（Ｓ６１８）。利用者１２のパーソナルコンピュータ４０または携帯電話機１３においては、モデム４０４または送受信部１３５が仮想店舗２４から送信された受注取消を受信し（Ｓ３１５）、その旨を表示装置４０６または１３７に表示する（Ｓ３１６）。

上記第３の実施の形態は仮想口座１１０を決済機関９０に設けている点で上記第１および第２の実施の形態と大きく相違するが、その他の点でも相違している。これらの相違点は上記第１および第２の実施の形態でも採用することは可能であ

APPL-1002
APPLE INC. / Page 710 of 1892

る。

［第４の実施の形態］

上記第３の実施の形態では携帯電話会社１０に設けた個人情報１１に基づいて利用者１２の認証を行なっているが、以下に述べる第４の実施の形態では決済機関９０に設けた利用者情報９１０に基づいて利用者１２の認証を行なう。この第４の実施の形態のためのハードウエア構成は、図４７、図４９、図５３、図５７および図６２に示したものと同じであるから、その説明は繰返さない。以下、第４の実施の形態を上記第３の実施の形態との相違点を中心に説明する。

１．前払い方法

まず、仮想口座に入金する前払い方法について説明する。図６５は、この発明の第４の実施の形態に従う前払い方法を示す概略図である。ここでは、携帯電話機１３のＲＡＭ１３２内に、後述するワンタイムＩＤ、小口口座残高および小口決済履歴を記憶するための領域が確保されている。また、決済機関９０の利用者情報９１０には、利用者１２を認証するためのキーコードおよびパスワードが含まれている。利用者情報９１０にはまた、携帯電話機１３のメールアドレス、利用状況および会員区分が含まれている。会員区分には個人利用者の「一般」と「加盟店」とがある。仮想口座１１０には、小口口座残高およびワンタイムＩＤが含まれている。図６６および図６７は、図６５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

まず、利用者１２は携帯電話機１３を用い、メニュー画面で「前払い」を選択する（Ｓ９８）。具体的には、図４７、図４９、図５３、図５７および図６２に示した携帯電話機１３において、利用者１２の操作に応じて入力装置１３６が「前払い」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３は図５０に示したものと同じであるから、その説明は繰返さない。

パスワードの検証（Ｓ１０２）後、利用者１２は携帯電話機１３を用い、予め付与されている顧客番号を入力する（Ｓ１７５）。具体的には、利用者１２の操作に応じて入力装置１３６が入力された顧客番号をデータ処理部１３１に与える。ここでは利用者１２が顧客番号を入力しているが、最初に入力された顧客番号を

ＲＡＭ１３２に記憶しておき、２回目以降はこの記憶された顧客番号を送信するようにしてもよい。また、上記実施の形態のように携帯電話機１３の電話番号を顧客番号として用いてもよい。

続いて、携帯電話機１３の送受信部１３５がステップＳ１７５で入力された顧客番号、ＲＯＭ１３３に予め登録されているキーコード、およびステップＳ１０１で入力されたパスワードを携帯電話会社１０に送信する（Ｓ１７６）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された顧客番号、キーコードおよびパスワードを受信し、これらをそのままインターネット６０を介して決済機関９０に送信する。すなわち、携帯電話会社１０は携帯電話機１３から送信された顧客番号、キーコードおよびパスワードを決済機関９０に転送する（Ｓ２６５）。

決済機関９０のサーバ９２においては、携帯電話機１３から携帯電話会社１０を介して送信された顧客番号、キーコードおよびパスワードをデータ処理部９２１が受信する（Ｓ２００）。以降、決済機関９０のサーバ９２は、図５０および図５１に示したステップＳ２０３～Ｓ２０５，Ｓ２５０，Ｓ２５１と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。但しここでは、決済機関９０のサーバ９２は認証異常通知を携帯電話会社１０に送信し、携帯電話会社１０のサーバ３０はこれを携帯電話機１３に転送する（Ｓ２６６）。また、決済機関９０のサーバ９２は利用不可通知を携帯電話会社１０に送信し、携帯電話会社１０のサーバ３０はこれを携帯電話機１３に転送する（Ｓ２６７）。携帯電話機１３のステップＳ１５０～Ｓ１５２，Ｓ１１０，Ｓ１１１は図５１に示したものと同じであるから、その説明は繰返さない。

利用状況の確認（Ｓ２０４）の結果、利用状況が「利用可」の場合、決済機関９０は利用者１２に対して前払金額の入力を要求する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が前払金額の要求を携帯電話機１３に送信する（Ｓ１３４０）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された前払金額の要求を利用者１２の携帯電話機１３に転送する（Ｓ２６８）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から

携帯電話会社１０を介して送信された前払金額の要求を受信する（Ｓ１７７）。

利用者１２はこの要求に応じて携帯電話機１３の入力装置１３６を操作し、所望の前払金額を入力するとともに前払金額の支払方法を選択する（Ｓ１７８）。この支払方法としては、上記と同様に銀行口座からの引落し、デビット決済、クレジット決済の他、振込み、電子マネーによる決済などがある。携帯電話機１３の送受信部１３５は、この入力された前払金額および選択された支払方法を決済機関９０に送信する。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された前払金額および支払方法を決済機関９０に転送する（Ｓ２６９）。

決済機関９０のサーバ９２においては、携帯電話機１３から携帯電話会社１０を介して送信された前払金額および支払方法をデータ処理部９２１が受信する（Ｓ１３４１）。

続いて、データ処理部９２１は選択された支払方法で所望の前払金額の決済処理を実行する（Ｓ１３４２）。

続いて、データ処理部９２１は決済が可能か否かを判定する（Ｓ１３４３）。決済が不可能な場合、決済機関９０は利用者１２に前払不可を通知する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が前払不可の通知を携帯電話機１３に送信する（Ｓ１３４４）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された前払不可の通知を携帯電話機１３に転送する（Ｓ２７０）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された前払不可の通知を受信し（Ｓ１７９）、前払不可を表示装置１３７に表示する（Ｓ１８０）。

一方、ステップＳ１３４３で決済が可能な場合、決済機関９０は利用者１２に仮想口座の新しい残高とともに前払完了を通知する。具体的には、データ処理部９２１が仮想口座の残高とともに前払完了の通知を携帯電話機１３に送信する（Ｓ１３４５）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された仮想口座の残高および前払完了の通知を利用者１２の携帯電話機１３に転送する（Ｓ２７１）。

APPL-1002
APPLE INC. / Page 713 of 1892

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された仮想口座の残高および前払完了の通知を受信し（Ｓ１８１）、データ処理部１３１が仮想口座の残高とともに前払完了を表示装置１３７に表示する（Ｓ１８２）。

前払完了の通知（Ｓ１３４５）後、データ処理部９２１は前払金額に基づいて入出金履歴９１２を更新し（Ｓ１３０６）、さらに仮想口座１１０の残高を更新する（Ｓ１３０８）。

上述したステップＳ２６５～Ｓ２７１に係る通信は同一セッション内で行なわれる。したがって、入出金履歴や仮想口座残高を更新する前に通信が遮断された場合は入出金履歴や仮想口座残高は更新されない。

２．仮想店舗での決済

次に、仮想店舗での決済について説明する。以下に仮想口座から仮想店舗に請求金額を送金する２つの方法を挙げる。

２－１．第１の送金方法

図６８は、この発明の第４の実施の形態に従う第１の送金方法を示す概念図である。ここでは、決済機関９０のサーバ９２に設けられたデータベース９２２に、加盟店請求履歴９１８および加盟店入金履歴９２０が記録される。図６９および図７０は、図６８に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

上記第３の実施の形態と同様に、利用者１２のパーソナルコンピュータ４０または携帯電話機１３は注文内容とともに顧客番号を仮想店舗２４に送信する（Ｓ３０１）。仮想店舗２４のサーバ５０はこれらを受信し（Ｓ６０１）、顧客番号とともに請求内容を決済機関９０に送信する（Ｓ６０２）。

決済機関９０のサーバ９２においては、データ処理部９２１が仮想店舗２４から送信された請求内容を受信する（Ｓ１３１０）。

続いて、決済機関９０のサーバ９２は、図５４に示したステップＳ５０２，Ｓ５０３，Ｓ５０５と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。但しここでは、携帯電話番号の代わりに顧客番号に基づいて決済機関９０の

サーバ９２がデータベース９２２中の利用者情報９１０を検索する（Ｓ５０２）。

利用状況の確認（Ｓ５０３）の結果、利用状況が「利用可」の場合、決済機関９０のサーバ９２においては、データ処理部９２１が顧客番号に基づいてデータベース９２２を検索し、利用者情報９１０の中から携帯電話機１３の電子メールアドレスを読出し、その電子メールアドレスに従って電子請求書を電子メールで携帯電話機１３に送信する（Ｓ５０５）。この電子請求書には、請求番号、請求金額、送金先（加盟店番号）などが記録されている。

続いて、データ処理部９２１は加盟店請求履歴９１８を更新し、仮想店舗２４から送信された電子請求書に基づいて、請求番号、請求日、請求金額などを記録する（Ｓ１３４０）。

携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された電子メールを利用者１２の携帯電話機１３に転送する（Ｓ２７２）。

携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された電子メールを受信し（Ｓ４０１）、データ処理部１３１が利用者１２の操作に応じて電子メールを開封し、電子請求書を表示装置１３７に表示する（Ｓ４１８）。

続いて、利用者１２が電子請求書を確認し、そこに記録されている請求金額を仮想店舗２４に送金する場合は「送金」を選択する。このとき、利用者１２は入力装置１３６を操作して顧客番号およびパスワードも入力する。これにより携帯電話機１３は電子メールに埋込まれている送金ＵＲＬ(Uniform Resource Locator)に従って決済機関９０のサーバ９２に接続され、送受信部１３５がキーコード、顧客番号およびパスワードとともに送金選択信号を決済機関９０に送信する（Ｓ４３０）。携帯電話会社１０のサーバ３０は、携帯電話機１３から送信された送金選択信号をインターネット６０を介して決済機関９０に転送する（Ｓ２７３）。

決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話機１３から携帯電話会社１０を介して送信されたキーコード、顧客番号、パスワードおよび送金選択信号を受信し（Ｓ１３４１）、その受信した顧客番号に基づいてデ

APPL-1002
APPLE INC. / Page 715 of 1892

ータベース９２２中の利用者情報９１０を検索する（Ｓ１３４２）。以降、決済機関９０のサーバ９２は図５５に示したステップＳ５１１，Ｓ５１２，Ｓ５２２～Ｓ５２４と同じ処理を携帯電話会社１０のサーバ３０に代わって実行する。

データ処理部９２１がキーコードおよびパスワードを検証し（Ｓ５１１，Ｓ５１２）、両方共一致した場合は仮想口座１１０の新しい残高とともに送金完了の通知を携帯電話会社１０を介して利用者１２の携帯電話機１３に送信する（Ｓ１３４３）。携帯電話会社１０のサーバ３０は、決済機関９０からインターネット６０を介して送信された送金完了の通知を利用者１２の携帯電話機１３に転送する（Ｓ２７５）。携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された送金完了通知を受信し（Ｓ４３１）、さらにデータ処理部１３１が送金後の仮想口座残高とともに送金完了を表示装置１３７に表示する（Ｓ４３２）。

送金完了の通知（Ｓ１３４３）後、決済機関９０のサーバ９２は図５６に示したステップＳ１３２０～Ｓ１３２２と同じ処理を実行する。

仮想口座残高の更新（Ｓ１３２２）後、データ処理部９２１はデータベース９２２中の加盟店請求履歴９１８を更新し、入金日を記録する（Ｓ１３４４）。

続いて、データ処理部９２１はデータベース９２２中の加盟店入金履歴９２０を更新し、請求番号、入金日、入金額、送金顧客番号などを記録する（Ｓ１３４５）。

続いて、データ処理部９２１は入金通知をインターネット６０を介して仮想店舗２４に送信する（Ｓ１３４６）。仮想店舗２４のサーバ５０においては、モデム５０４が決済機関９０から送信された入金通知を受信する（Ｓ６１９）。

ここでは、ステップＳ２７２～Ｓ２７５に係る通信は同一セッション内で行なわれる。

２－２．第２の送金方法

図７１は、この発明の第４の実施の形態に従う第２の送金方法を示す概念図である。図７２および図７３は、図７１に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

APPL-1002
APPLE INC. / Page 716 of 1892

注文を受けた仮想店舗２４は、上記第１の送金方法のように支払内容を決済機関９０を介して利用者１２に通知するのではなく、ここでは支払内容を利用者１２に直接通知する。具体的には、仮想店舗２４のサーバ５０においては、注文の受信（Ｓ６０１）後、データ処理部５０１は仮想店舗２４の加盟店番号と請求金額などの請求内容をインターネット６０を介して利用者１２の携帯電話機１３またはパーソナルコンピュータ４０に送信する（Ｓ６２０）。利用者１２の携帯電話機１３またはパーソナルコンピュータ４０においては、送受信部１３５またはモデム４０４がこれらを受信する（Ｓ３１２）。

利用者１２は通知された請求内容を見て携帯電話機１３を操作し、メニュー画面から「送金」を選択する（Ｓ９７）。図６６に示したステップＳ９９～１０３，Ｓ１７５，Ｓ１７６，Ｓ２６５，Ｓ２００と同様に、利用者１２はパスワードおよび顧客番号を入力し、携帯電話機１３はこれらをキーコードとともに決済機関９０に送信し、決済機関１２はこれらを受信する。

続いて、図６９に示したステップＳ５０２，Ｓ５０３，Ｓ１３１４，Ｓ６０３，Ｓ６０４，Ｓ３０２，Ｓ３０３，Ｓ５１１，Ｓ５１２，Ｓ５２２～Ｓ５２４，Ｓ２７４，Ｓ１５９，Ｓ６１３と同様に、決済機関９０は認証を行ない、ステップＳ５１１，Ｓ５１２でキーコードおよびパスワードの両方が一致した場合、具体的な送金内容を入力するよう利用者１２に要求する。利用者１２はこの要求に応じて具体的な送金内容を入力して決済機関９０に送信する。

具体的には、決済機関９０のサーバ９２においては、データ処理部９２１が送金内容の要求を利用者１２の携帯電話機１３に送信する（Ｓ１３４７）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された送金内容の要求を携帯電話機１３に転送する（Ｓ２７６）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された送金内容の要求を受信する（Ｓ４３３）。

続いて、入力装置１３６は利用者１２の操作に応じて入力された送金内容をデータ処理部１３１に与え、送受信部１３５はその入力された送金内容を決済機関９０に送信する（Ｓ４３４）。送金内容としては、送金先の加盟店番号、送金金

額などがある。携帯電話会社１０のサーバ３０においては、データ処理部３０１が携帯電話機１３から送信された送金内容を決済機関９０に転送する（Ｓ２７７）。決済機関９０のサーバ９２においては、データ処理部９２１が携帯電話機１３から携帯電話会社１０を介して送信された送金内容を受信する（Ｓ１３４８）。以降は、図７０に示したステップＳ１３４３，Ｓ２７５，Ｓ４３１，Ｓ４３２，Ｓ１３２０～Ｓ１３２２；Ｓ１３４５，Ｓ１３４６，Ｓ６１９と同じであるから、その説明は繰返さない。ただしここでは、図６８に示した請求履歴９１８はないので請求履歴の更新（Ｓ１３４４）は行なわれない。

３．実在店舗での決済

次に、実在店舗での決済について説明する。ここでは、仮想口座からの振替えが可能な小口口座をさらに設け、その小口口座の使用を可能にするワンタイムＩＤ（識別子）を発行する。

３－１．ワンタイムＩＤの発行（小口口座への振替え）

図７４および図７５は、この発明の第４の実施の形態に従ってワンタイムＩＤの発行方法を示す概念図である。図７４は小口決済履歴がない場合を示し、図７５は小口決済履歴がある場合を示す。ここでは、決済機関９０のサーバ９２に設けられたデータベース９２２に、小口口座の入出金履歴９１５が記録される。図７６および図７７は、図７４および図７５に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

実在店舗で決済をするために仮想口座から小口口座に所望の金額を振替えようとする場合、利用者１２は携帯電話機１３を操作し、メニュー画面で「ワンタイムＩＤ」を選択する（Ｓ９６）。具体的には、携帯電話機１３において、入力装置１３６が利用者１２の操作に応じて「ワンタイムＩＤ」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３，Ｓ１７５は図６６に示したものと同じであるから、その説明は繰返さない。

顧客番号の入力（Ｓ１７５）後、携帯電話機１３においては、送受信部１３５が顧客番号、キーコード、パスワードおよび小口口座情報を決済機関９０に送信する（Ｓ１８５）。小口口座情報には、ＲＡＭ１３２に記録されている小口口座

APPL-1002
APPLE INC. / Page 718 of 1892

残高および小口決済履歴が含まれる。但し、初めてワンタイムＩＤを要求する場合、小口決済履歴はまだ存在していない。以降、ステップＳ２６５～Ｓ２６７，Ｓ２００，Ｓ２０２～Ｓ２０５，Ｓ２５０，Ｓ２５１，Ｓ１５０～Ｓ１５２，Ｓ１１０，Ｓ１１１は図６６に示したものと同じであるから、その説明は繰返さない。

利用者１２の認証（Ｓ２０３）の結果、キーコードおよびパスワードが共に一致し、かつ利用状況の確認（Ｓ２０４）の結果、利用状況が「利用可」の場合、決済機関９０は利用者１２に対して仮想口座から小口口座への振替金額を要求する。具体的には、決済機関９０のサーバ９２において、データ処理部９２１が小口口座への希望振替金額の要求を利用者１２の携帯電話機１３に送信する（Ｓ１３５０）。このとき、振替可能な限度額（通常は仮想口座の残高）も併せて送信する。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された振替金額の要求を携帯電話機１３に転送する（Ｓ２７８）。

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された振替金額の要求を受信する（Ｓ１８６）。

この要求に応じ、利用者１２は携帯電話機１３の入力装置１３６を操作して所望の振替金額を指定する（Ｓ１８７）。入力装置１３６は利用者１２により指定された振替金額をデータ処理部１３１に与える。

データ処理部１３１はステップＳ１８７で指定された決済金額をステップＳ１８６で受信した限度額と比較し、指定された決済金額が限度額以内か否かを判定する（Ｓ１８８）。指定された振替金額が限度額を超えている場合、データ処理部１３１は振替不可を表示装置１３７に表示する（Ｓ１８９）。一方、指定された振替金額が限度額以内の場合、送受信部１３５はその指定された振替金額を決済機関９０に送信する（Ｓ１９０）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が利用者１２の携帯電話機１３から送信された振替金額をインターネット６０を介して決済機関９０に転送する（Ｓ２７９）。

決済機関９０のサーバ９２においては、データ処理部９２１が利用者１２の携帯電話機１３から携帯電話会社１０を介して送信された振替金額を受信し（Ｓ１

３５１）、さらにランダムにワンタイムＩＤを生成する（Ｓ１３５２）。

続いて、データ処理部９２１はステップＳ１３５１で受信した振替金額に基づいて、仮想口座の入出金履歴９１２を更新し（Ｓ１３２０）、仮想口座の決済履歴９１４を更新し（Ｓ１３２１）、仮想口座１１０の残高を更新し（Ｓ１３２２）、さらに小口口座の入出金履歴９１５を更新する（Ｓ１３４５）。

たとえば図７４に示すように利用者１２が振替金額を１０００円に指定した場合、仮想口座の入出金履歴９１２には１０００円が小口口座に出金された旨が記録される。また、仮想口座１１０の残高は１０００円減額され、小口口座の残高は１０００円増額される。さらに、小口口座の入出力履歴９１５には１０００円が入金された旨が記録される。この場合、小口決済履歴は携帯電話機１３から送信されて来ないので、仮想口座の決済履歴９１４は更新されない。

次に、図７５に示すように携帯電話機１３の小口決済履歴に３００円を使用した旨が記録されている（つまり携帯電話機１３の小口口座残高が７００円になっている）場合において利用者１２が振替金額を１５００円に指定したときは、この振替金額（１５００円）と現在の小口口座残高（７００円）との差額（８００円）が計算され、仮想口座の入出力履歴９１２には８００円が出金された旨が記録される。また、携帯電話機１３の小口決済履歴に基づいて仮想口座の決済履歴９１４には３００円が決済に使用された旨が記録される。また、上記差額に基づいて仮想口座１１０の残高は８００円減額され、２００円になる。小口口座から３００円が決済に使用されたが、新たに８００円が小口口座に振替えられるので、小口口座の残高は上記振替金額に等しい１５００円になる。また、小口口座の入出金履歴９１５には携帯電話機１３の小口決済履歴に基づいて３００円が出金された旨が記録され、さらに上記差額に基づいて８００円が入金された旨が記録される。

最後に、データ処理部９２１はステップＳ１３５２で生成したワンタイムＩＤや小口口座残高などの振替内容を利用者１２の携帯電話機１３に送信する（Ｓ１３５３）。携帯電話会社１０のサーバ３０においては、データ処理部３０１が決済機関９０からインターネット６０を介して送信された振替内容を携帯電話機１３に転送する（Ｓ２８０）。

APPL-1002
APPLE INC. / Page 720 of 1892

利用者１２の携帯電話機１３においては、送受信部１３５が決済機関９０から携帯電話会社１０を介して送信された振替内容を受信する（Ｓ１１９）。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口決済履歴をクリアする（Ｓ１９２）。続いて、データ処理部１３１は、ＲＡＭ１３２に記録されている小口口座残高を書替え（Ｓ１９３）、さらにＲＡＭ１３２に記録されているワンタイムＩＤを書替える（Ｓ１９４）。

たとえば図７４に示した場合、決済機関９０で生成された「９８７６５」のワンタイムＩＤが携帯電話機１３のＲＡＭ１３２に記録される。また、利用者１２が指定した振替金額に従って小口口座残高が「０円」から「１０００円」に更新される。また、図７５に示した場合、決済機関９０で生成された「３４５６７」の新しいワンタイムＩＤが携帯電話機１３のＲＡＭ１３２に記録される。また、決済機関９０で計算された「１５００円」の新しい小口口座残高が携帯電話機１３のＲＡＭ１３２に記録される。

最後に、データ処理部１３１は小口口座残高とともに小口口座への入金完了を表示装置１３７に表示する（Ｓ１９５）。

３－２．ワンタイムＩＤの使用（小口口座からの支払い）

図７８は、この発明の第４の実施の形態に従い、ワンタイムＩＤを使用して実在店舗で決済する方法を示す概念図である。図７９は、図７８に示した場合における、携帯電話機、実在店舗のＰＯＳ端末、および決済機関のサーバの動作を示すフローチャートである。

小口口座に所望の金額を振替えてワンタイムＩＤを獲得した後、実在店舗２６で決済を行なう場合、利用者１２は携帯電話機１３を操作し、メニュー画面で「支払い」を選択する（Ｓ９５）。具体的には、携帯電話機１３において、入力装置１３６が利用者１２の操作に応じて「支払い」の選択信号をデータ処理部１３１に与える。以降、ステップＳ９９～Ｓ１０３は図６６に示したものと同じであるから、その説明は繰返さない。

パスワードの検証（Ｓ１０２）後、データ処理部１３１はＲＡＭ１３２に記録されているワンタイムＩＤが有効か否かを判定する（Ｓ７３５）。ワンタイムＩＤには有効日が付与されており、小口口座の残高はその有効日までしか実在店舗

での決済に使用することができない。ワンタイムＩＤは実在店舗での決済に１回使用すれば無効になるようにしてもよい。

ワンタイムＩＤが無効な場合、データ処理部１３１はその旨を表示装置１３７に表示する（Ｓ７３６）。一方、ワンタイムＩＤが有効な場合、データ処理部１３１は小口口座からの支払いが可能である旨を表示装置１３７に表示する（Ｓ７３７）。以降、ステップＳ７１６～Ｓ７１９，Ｓ８０１は図5･9に示したものと同じであるから、その説明は繰返さない。

残高検証（Ｓ７１８）の結果、ＰＯＳ端末２７から送信された決済金額が小口口座の残高以内の場合、携帯電話機１３のインターフェイス部１３９はＰＯＳ端末２７にＲＡＭ１３２に記録されているワンタイムＩＤを送信する（Ｓ７３８）。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口決済履歴を更新する（Ｓ７３９）。具体的には、データ処理部１３１は、ＰＯＳ端末２７から送信された決済金額、決済日、実在店舗２６の加盟店番号などを記憶する。

続いて、データ処理部１３１はＲＡＭ１３２に記録されている小口口座の残高を更新する（Ｓ７４０）。具体的には、データ処理部１３１は、小口口座の残高から決済金額を減算して新しい残高を記録する。この時点で、携帯電話機１３の小口口座の残高は決済機関９０の小口口座の残高とずれる。

最後に、データ処理部１３１は小口口座の新しい残高とともに決済の完了を表示装置１３７に表示する（Ｓ７４１）。

実在店舗２６のＰＯＳ端末２７においては、インターフェイス部２７６が携帯電話機１３から送信されたワンタイムＩＤを受信する（Ｓ８１０）。

続いて、データ処理部２７１はその決済金額に基づいて売上計上処理を実行する（Ｓ８１１）。

続いて、インターフェイス部２７６は、加盟店番号とともにワンタイムＩＤ、決済日、決済金額、顧客番号などの決済内容を決済機関９０に送信する（Ｓ８０５）。

決済機関９０のサーバ９２においては、データ処理部９２１がＰＯＳ端末２７から送信された決済内容を受信し（Ｓ１３３３）、その受信した決済内容に基づいて加盟店の入金履歴９２０を更新する（Ｓ１３５５）。

続いて、データ処理部９２１はその支払を承認した旨の通知を実在店舗２６に送信する（Ｓ１３２４）。実在店舗２６のＰＯＳ端末２７は、決済機関９０から送信された支払承認の通知を受信する（Ｓ８０６）。

最後に、データ処理部９２１はたとえば月末に１ヶ月間の総支払金額を計算し、実在店舗２６に対する支払処理を実行する（Ｓ１３２５）。

上述した第４の実施の形態では、携帯電話会社１０のサーバ３０が携帯電話機１３から送信されたキーコードをそのまま決済機関９０のサーバ９２に転送しているが、携帯電話機１３から送信されたキーコードをこれと１対１に対応する別のキーコードに変換して決済機関９０のサーバ９２に送信するようにしてもよい。

また、小口口座への振替えの際にワンタイムＩＤをダウンロードするようにしているが、利用者１２が携帯電話機１３で決済機関９０が提供するサービスサイトにアクセスする度に自動的に新しいワンタイムＩＤをダウンロードするようにしてもよい。この場合、ワンタイムＩＤの更新頻度が増すため、セキュリティがさらに高くなる。

また、ワンタイムＩＤを１次元または２次元バーコードのイメージとし、実在店舗での決済の際には携帯電話機１３に表示されたバーコードをＰＯＳ端末２７のリーダで光学的に読取るようにしてもよい。この場合、携帯電話機１３から情報を読取るための専用機器をＰＯＳ端末２７に取付ける必要はなく、既存のバーコードリーダを用いればよい。また、小口口座の残高をワンタイムＩＤのバーコードに付加してもよい。

この発明の第４の実施の形態によれば、決済機関９０が携帯電話機１３から出力されるキーコードを取得し、利用者１２の認証を行なっているため、認証を携帯電話会社１０に依存することはない。そのため、決済会社９０だけで本サービスを提供することができる。

また、仮想口座とは別に小口口座を設け、実在店舗で決済する際には予め仮想口座から小口口座に振替えを行なっておき、小口口座から代金を支払うようにしているため、上記第１～第２の実施の形態のように仮想口座の残高が真の残高からずれることはない。また、決済機関が小口口座からの出金を可能にするためのワンタイムＩＤを発行し、ワンタイムＩＤが有効でかつ決済金額が小口口座の残

APPL-1002
APPLE INC. / Page 723 of 1892

高以内の場合だけ携帯電話機１３からＰＯＳ端末２７にワンタイムＩＤが出力され、ＰＯＳ端末２７はこのワンタイムＩＤに基づいて決済を完了するようにしているため、セキュリティが高くなる。

上記各コンピュータには所定のプログラムがインストールされている。この各プログラムは、フローチャートで示した各列に並ぶ一連のステップを対応のコンピュータに実行させるためのものである。各プログラムはＣＤ－ＲＯＭのようなコンピュータ読取可能な媒体に記録して配布可能である。

今回開示された実施の形態はすべての点で例示であって制限的なものではないと解釈されるものである。本発明の範囲は上述した実施の形態ではなく特許請求の範囲によって定められ、特許請求の範囲と均等の意味およびその範囲内でのすべての変更が含まれることを意図するものである。

産業上の利用可能性

この発明は、携帯電話機を用いた決済サービスに適用可能である。

APPL-1002
APPLE INC. / Page 724 of 1892

請求の範囲

１．売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、前記利用者の金銭を蓄積するための第１の口座を有するコンピュータにおいて、

前記携帯電話機から送信された所望の金額を受信するステップと、

前記受信した所望の金額を前記利用者の第１の口座に入金してその口座の残高を更新するステップと、

前記更新した第１の口座の残高を前記携帯電話機に送信するステップと、

決済金額を受信するステップと、

前記受信した決済金額を前記第１の口座の残高から減じるステップと、

前記受信した決済金額を前記売り主に支払うステップとを含む、方法。

２．前記受信した所望の金額を前記利用者に対して課金するステップをさらに含む、請求項１に記載の方法。

３．前記携帯電話機から送信された識別情報を受信するステップと、

前記受信した識別情報に基づいて前記利用者の認証を行なうステップとをさらに含む、請求項１に記載の方法。

４．前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項３に記載の方法。

５．前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項４に記載の方法。

６．前記利用者固有情報はパスワードをさらに含む、請求項５に記載の方法。

７．前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項４に記載の方法。

８．前記利用者固有情報はパスワードをさらに含む、請求項７に記載の方法。

９．前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項４に記載の方法。

１０．前記電話機固有情報は前記携帯電話機の製造番号を含む、請求項９に記載の方法。

APPL-1002
APPLE INC. / Page 725 of 1892

１１．前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項９に記載の方法。

１２．前記サブスクライバ識別子は携帯電話局を介して送信される、請求項１１に記載の方法。

１３．前記コンピュータは第２の口座をさらに有し、

前記携帯電話機から送信された振替金額を受信するステップと、

前記受信した振替金額を前記第１の口座から前記第２の口座に振替えるステップと、

前記第２の口座の残高を使用可能にするためのワンタイム識別子を生成して前記携帯電話機に送信するステップとをさらに含む、請求項１に記載の方法。

１４．前記コンピュータは携帯電話会社に設けられる、請求項１に記載の方法。

１５．前記コンピュータは決済機関に設けられる、請求項１に記載の方法。

１６．前記コンピュータは金融機関に設けられる、請求項１に記載の方法。

１７．売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、前記利用者の金銭を蓄積するための口座を有する金融機関のコンピュータにおいて、

携帯電話局のコンピュータから決済金額を受信するステップと、

前記受信した決済金額を前記口座の残高から減じるステップと、

前記受信した決済金額を前記売り主に支払うステップとを含む、方法。

１８．前記携帯電話機から送信された金額を前記携帯電話局のコンピュータを介して受信するステップと、

前記受信した金額を前記利用者の口座に振替えてその口座の残高を更新するステップと、

前記更新した口座の残高を前記携帯電話局のコンピュータを介して前記携帯電話機に送信するステップとをさらに含む、請求項１７に記載の方法。

１９．売り主と携帯電話機の利用者たる買い主との間の決済に用いられ、前記利用者の金銭を蓄積するための第１の口座を有するコンピュータにアクセス可能な携帯電話機であって、

前記利用者の操作に応じて前記第１の口座に入金されるべき所望の金額を入力

APPL-1002
APPLE INC. / Page 726 of 1892

する入力手段と、

前記入力された金額を前記コンピュータに送信し、前記コンピュータから送信された前記第１の口座の残高を受信する送受信手段と、

前記受信した第１の口座の残高を記憶する手段とを備える、携帯電話機。

２０．前記送受信手段はさらに前記利用者の認証に必要な識別情報を前記コンピュータに送信する、請求項１９に記載の携帯電話機。

２１．前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項２０に記載の携帯電話機。

２２．前記利用者固有情報を記憶する手段をさらに備える、請求項２１に記載の携帯電話機。

２３．前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項２１に記載の携帯電話機。

２４．前記利用者固有情報はパスワードをさらに含む、請求項２３に記載の携帯電話機。

２５．前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項２１に記載の携帯電話機。

２６．前記利用者固有情報はパスワードをさらに含む、請求項２５に記載の携帯電話機。

２７．前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項２１に記載の携帯電話機。

２８．前記電話機固有情報を記憶する手段をさらに備える、請求項２７に記載の携帯電話機。

２９．前記電話機固有情報は携帯電話機の製造番号を含む、請求項２８に記載の携帯電話機。

３０．前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項２８に記載の携帯電話機。

３１．前記送受信手段はさらに決済金額を受信し、

前記送受信手段により受信された決済金額を記憶する手段をさらに備え、

前記送受信手段はさらに前記記憶された決済金額を読出して前記コンピュータ

に送信する、請求項１９に記載の携帯電話機。

３２．前記記憶された第１の口座の残高から前記記憶された決済金額を減算する手段をさらに備える、請求項３１に記載の携帯電話機。

３３．前記コンピュータは第２の口座をさらに有し、

前記入力手段は前記利用者の操作に応じて前記第１の口座から前記第２の口座に振替えられるべき振替金額を入力し、

前記送受信手段はさらに前記入力された振替金額を前記コンピュータに送信し、

前記送受信手段はさらに前記第２の口座の残高を使用可能にするためのワンタイム識別子を受信し、

前記ワンタイム識別子が有効か否かを判定する手段と、

前記ワンタイム識別子の判定の結果、前記ワンタイム識別子が有効な場合、前記送受信手段により受信された決済金額が前記第２の口座の残高以内か否かを判定する手段と、

前記決済金額の判定の結果、前記決済金額が前記第２の口座の残高以内の場合、前記受信したワンタイム識別子を出力する手段と、

前記決済金額を前記第２の口座から減じる手段とをさらに備える、請求項３１記載の携帯電話機。

FIG. 1

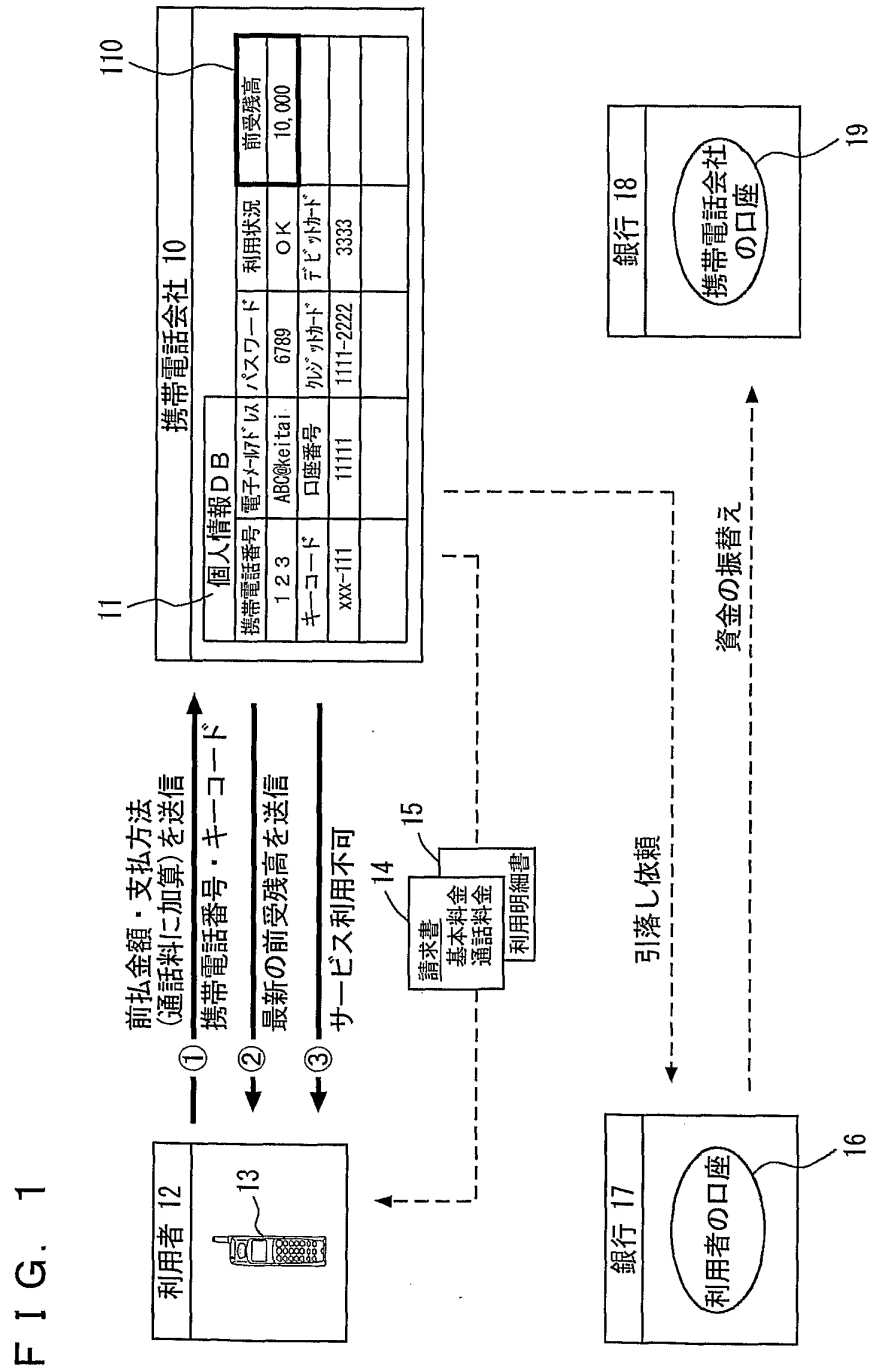
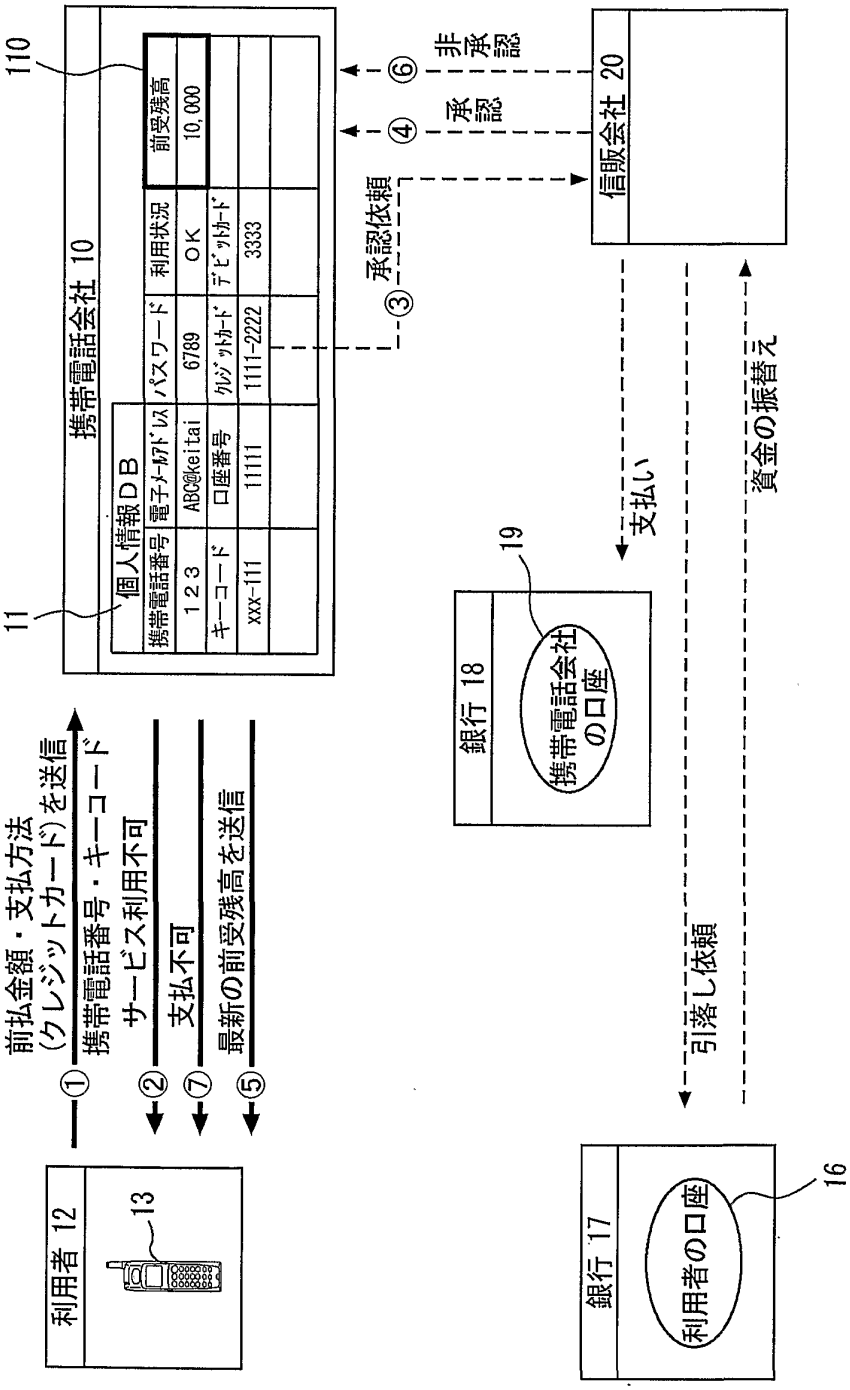

利用者 12
13
前払金額・支払方法
(通話料に加算)を送信
①携帯電話番号・キーコード
②最新の前受残高を送信
③サービス利用不可
14
15
請求書
基本料金
通話料金
利用明細書
携帯電話会社 10
110
11
個人情報DB
携帯電話番号
電子メールアドレス
パスワード
利用状況
前受残高
123
ABC@keitai
6789
OK
10,000
キーコード
口座番号
クレジットカード
デビットカード
xxx-111
11111
1111-2222
3333
引落し依頼
資金の振替え
銀行 17
利用者の口座
16
銀行 18
携帯電話会社の口座
19

FIG. 2



APPL-1002
APPLE INC. / Page 730 of 1892

FIG. 3

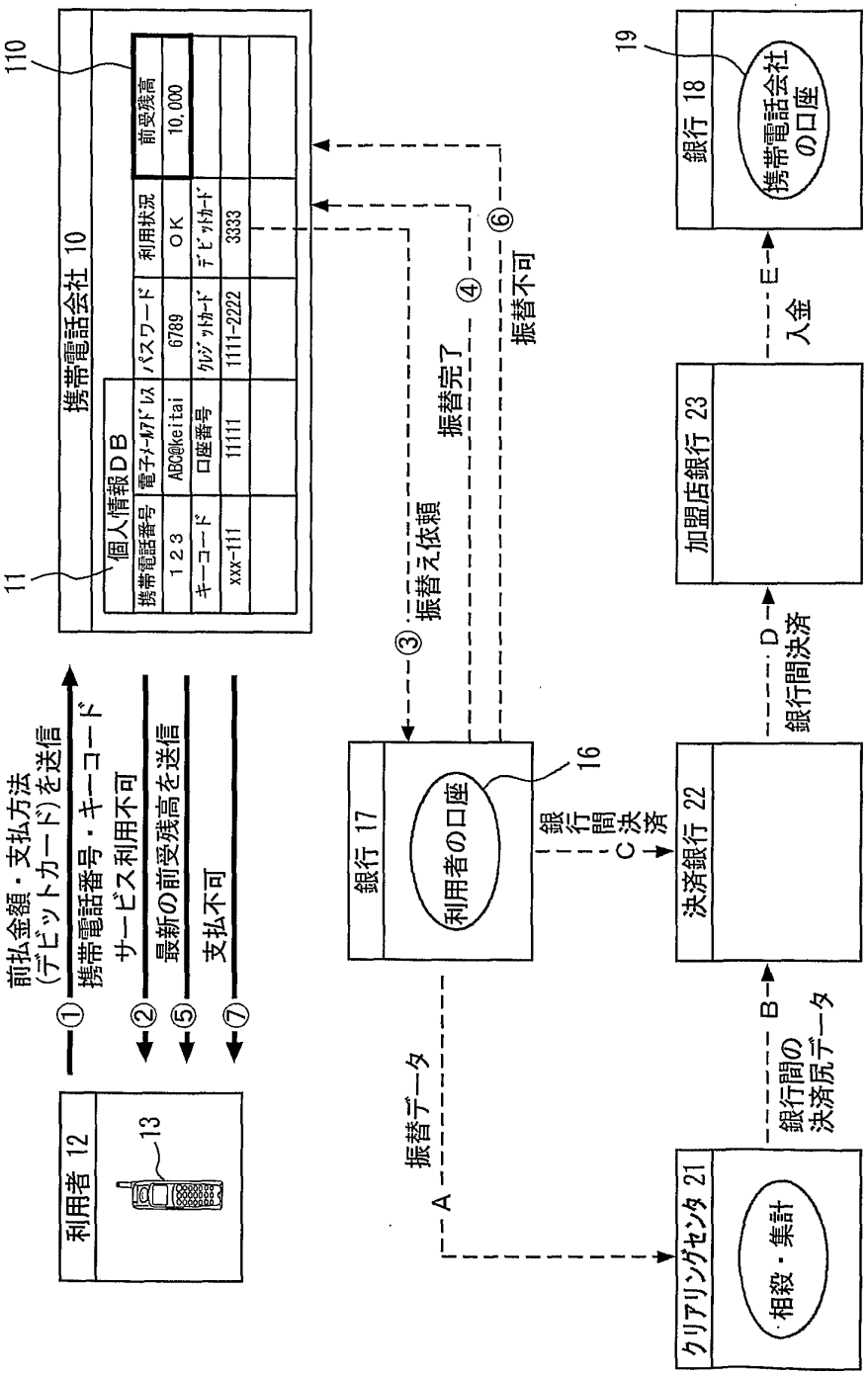

利用者 12
13
前払金額・支払方法
(デビットカード)を送信
①
携帯電話番号・キーコード
サービス利用不可
②
最新の前受残高を送信
⑤
支払不可
⑦
11
携帯電話会社 10
110
個人情報DB
携帯電話番号
電子ﾒｰﾙｱﾄﾞﾚｽ
ﾊﾟｽﾜｰﾄﾞ
利用状況
前受残高
123
ABC@keitai
6789
OK
10,000
キーコード
口座番号
ｸﾚｼﾞｯﾄｶｰﾄﾞ
ﾃﾞﾋﾞｯﾄｶｰﾄﾞ
xxx-111
11111
1111-2222
3333
③
振替え依頼
④
振替完了
⑥
振替不可
銀行 17
利用者の口座
16
銀行間C決済
振替データ
A
クリアリングセンタ 21
相殺・集計
銀行間の決済尻データ
B
決済銀行 22
D
銀行間決済
加盟店銀行 23
E
入金
19
銀行 18
携帯電話会社の口座

FIG. 4

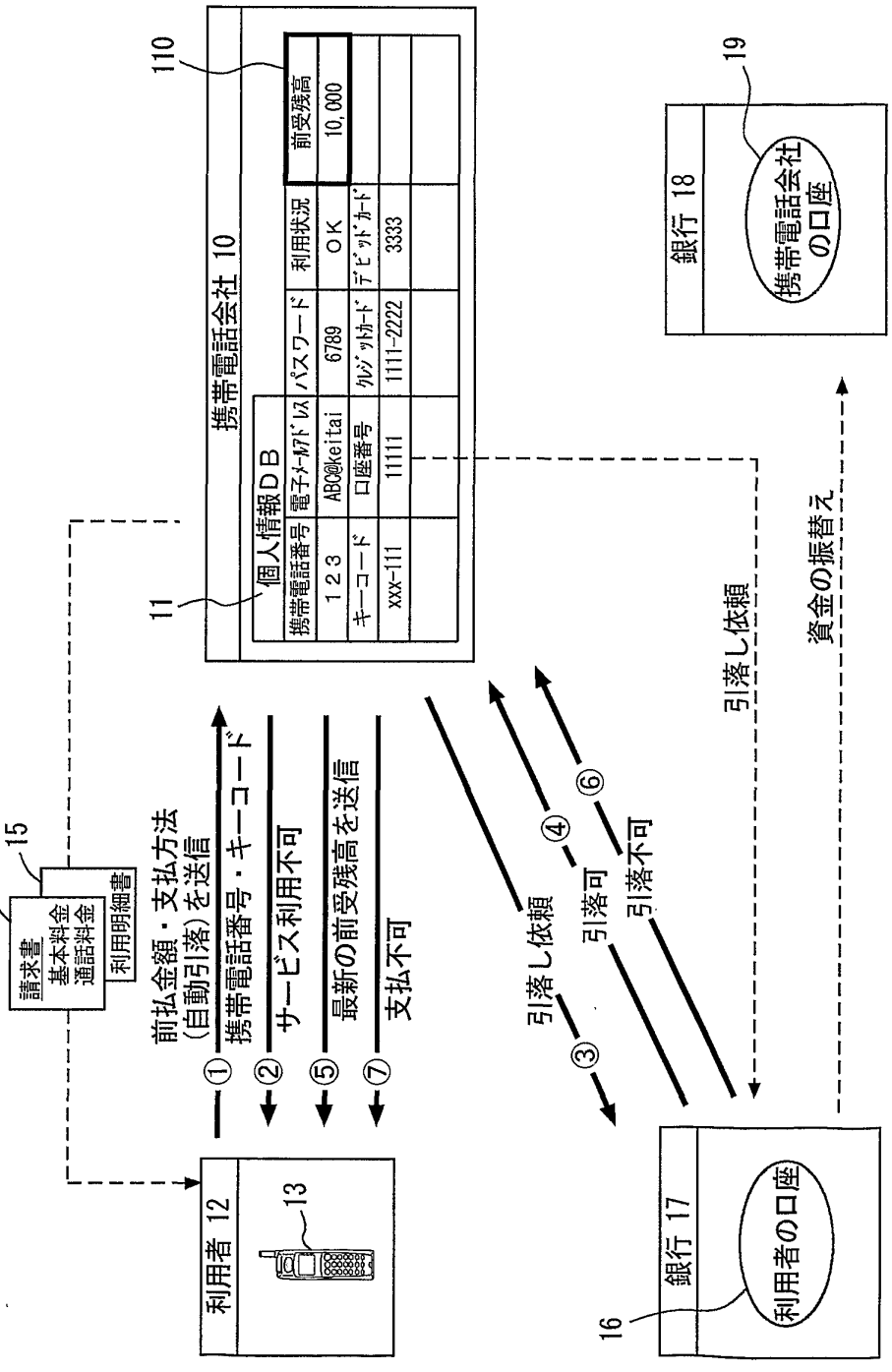
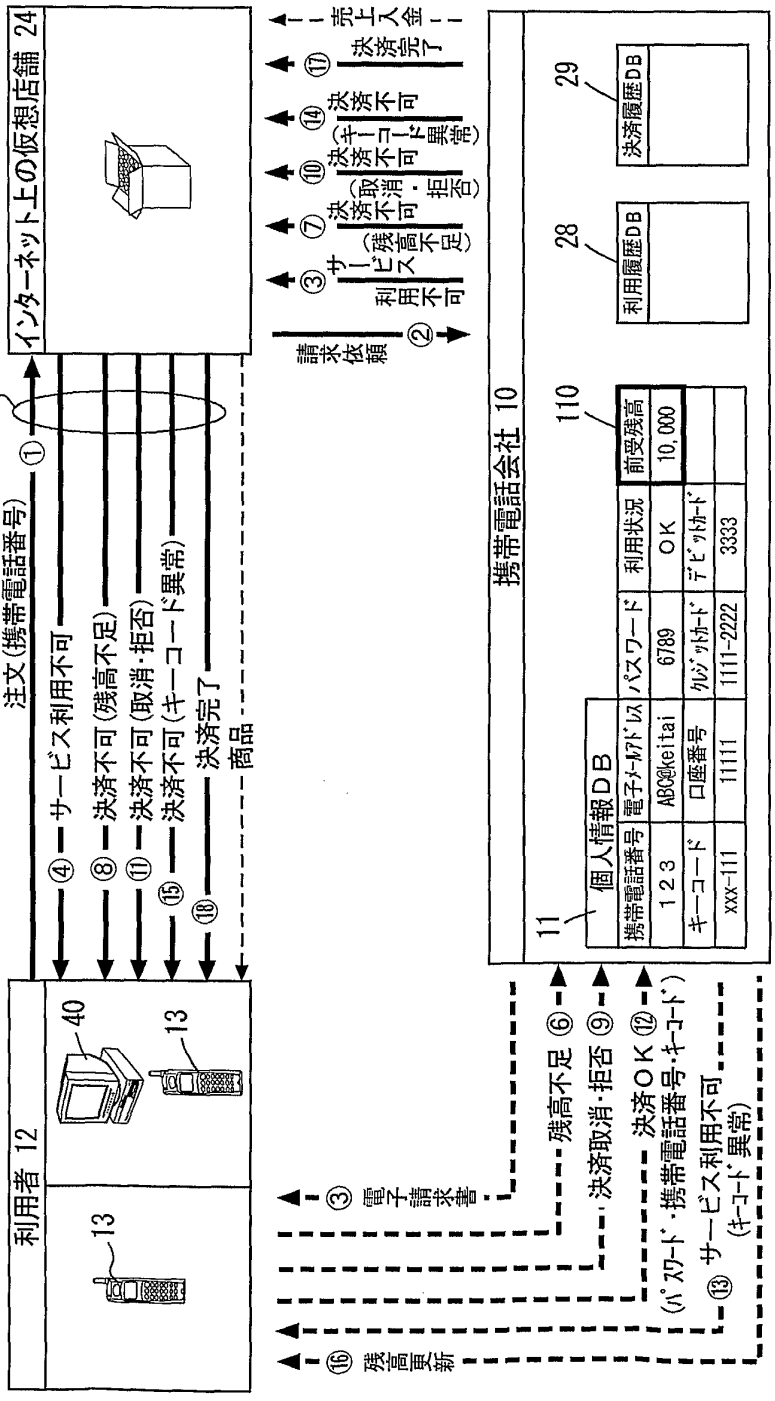

携帯電話会社 10
110
11
個人情報DB
携帯電話番号
電子ﾒｰﾙｱﾄﾞﾚｽ
ﾊﾟｽﾜｰﾄﾞ
利用状況
前受残高
123
ABC@keitai
6789
OK
10,000
キーコード
口座番号
ｸﾚｼﾞｯﾄｶｰﾄﾞ
ﾃﾞﾋﾞｯﾄﾄﾞｶｰﾄﾞ
xxx-111
11111
1111-2222
3333
利用者 12
13
請求書
基本料金
通話料金
利用明細書
14
15
銀行 17
利用者の口座
16
銀行 18
携帯電話会社の口座
19
前払金額・支払方法（自動引落）を送信
①
携帯電話番号・キーコード
②
サービス利用不可
⑤
最新の前受残高を送信
⑦
支払不可
引落し依頼
③
引落可
④
引落不可
⑥
引落し依頼
資金の振替え

FIG. 5



APPL-1002
APPLE INC. / Page 733 of 1892

FIG. 6

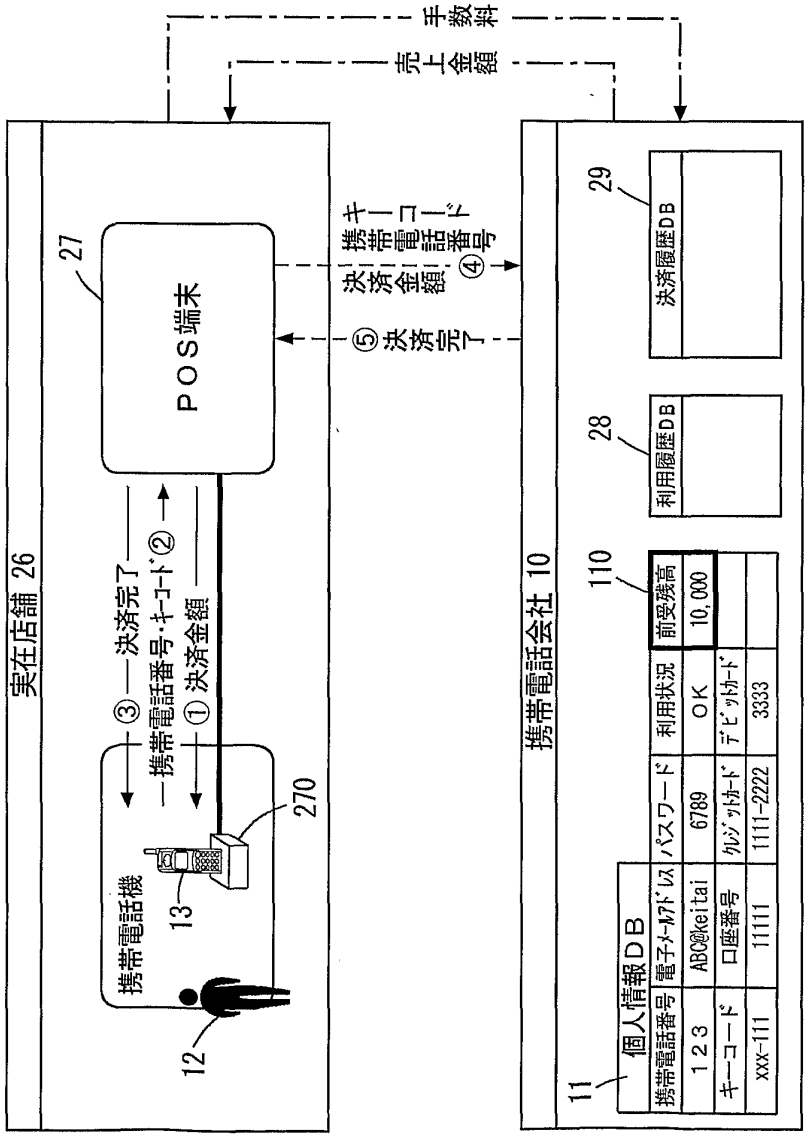

手数料
売上金額
実在店舗 26
27
POS端末
携帯電話機
13
270
12
③ 決済完了
携帯電話番号・キーコード②
① 決済金額
携帯キーコード
決済金額 ④携帯電話番号
⑤ 決済完了
携帯電話会社 10
11
個人情報DB
携帯電話番号 | 電子メールアドレス | パスワード | 利用状況
123 | ABC@keitai | 6789 | OK
キーコード | 口座番号 | クレジットカード | デビットカード
xxx-111 | 11111 | 1111-2222 | 3333
110
前受残高
10,000
28
利用履歴DB
29
決済履歴DB

FIG. 7

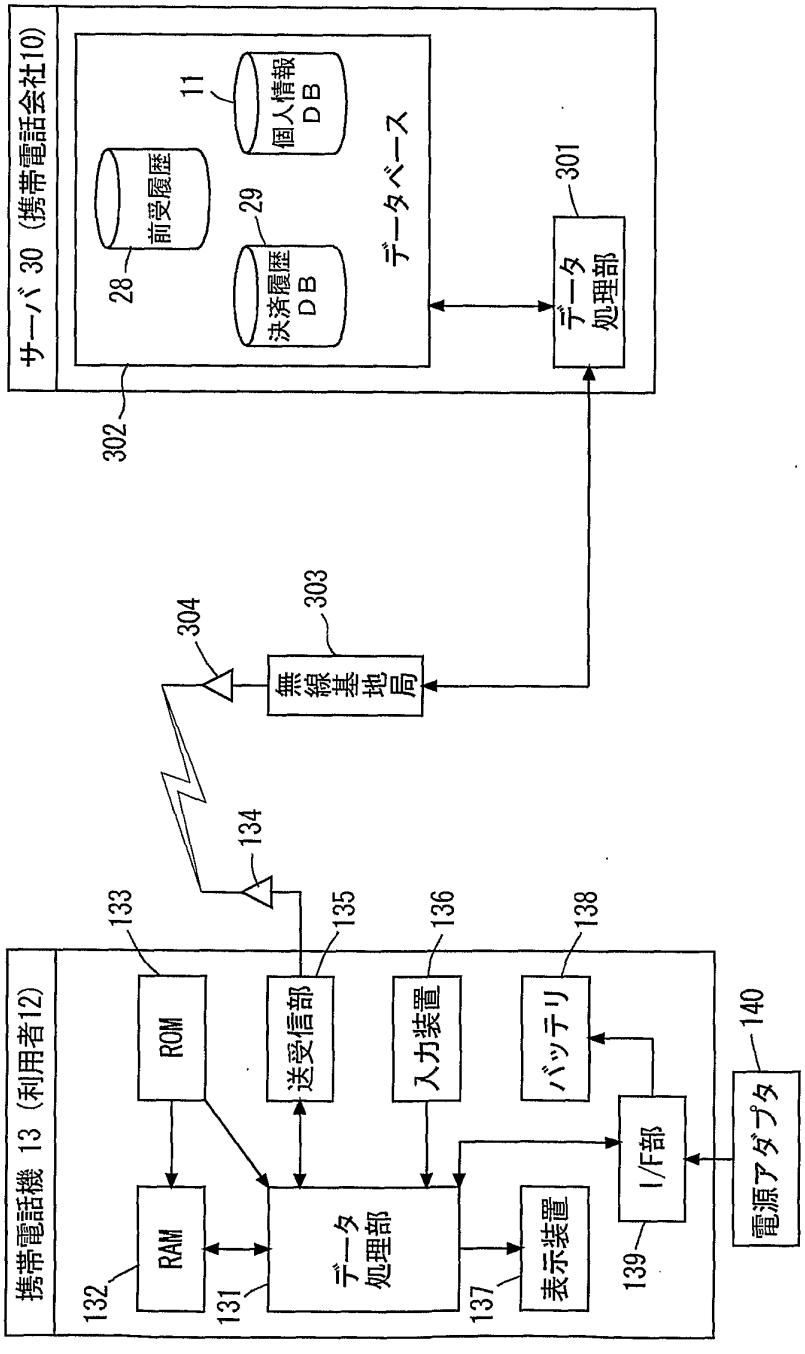

サーバ 30 (携帯電話会社10)
データベース
個人情報 DB
11
前受履歴
28
29
決済履歴 DB
データ 処理部
301
302
無線基地局
303
304
134
携帯電話機 13 (利用者12)
ROM
133
送受信部
135
入力装置
136
バッテリ
138
RAM
132
データ 処理部
131
表示装置
137
I/F部
139
電源アダプタ
140

FIG. 8

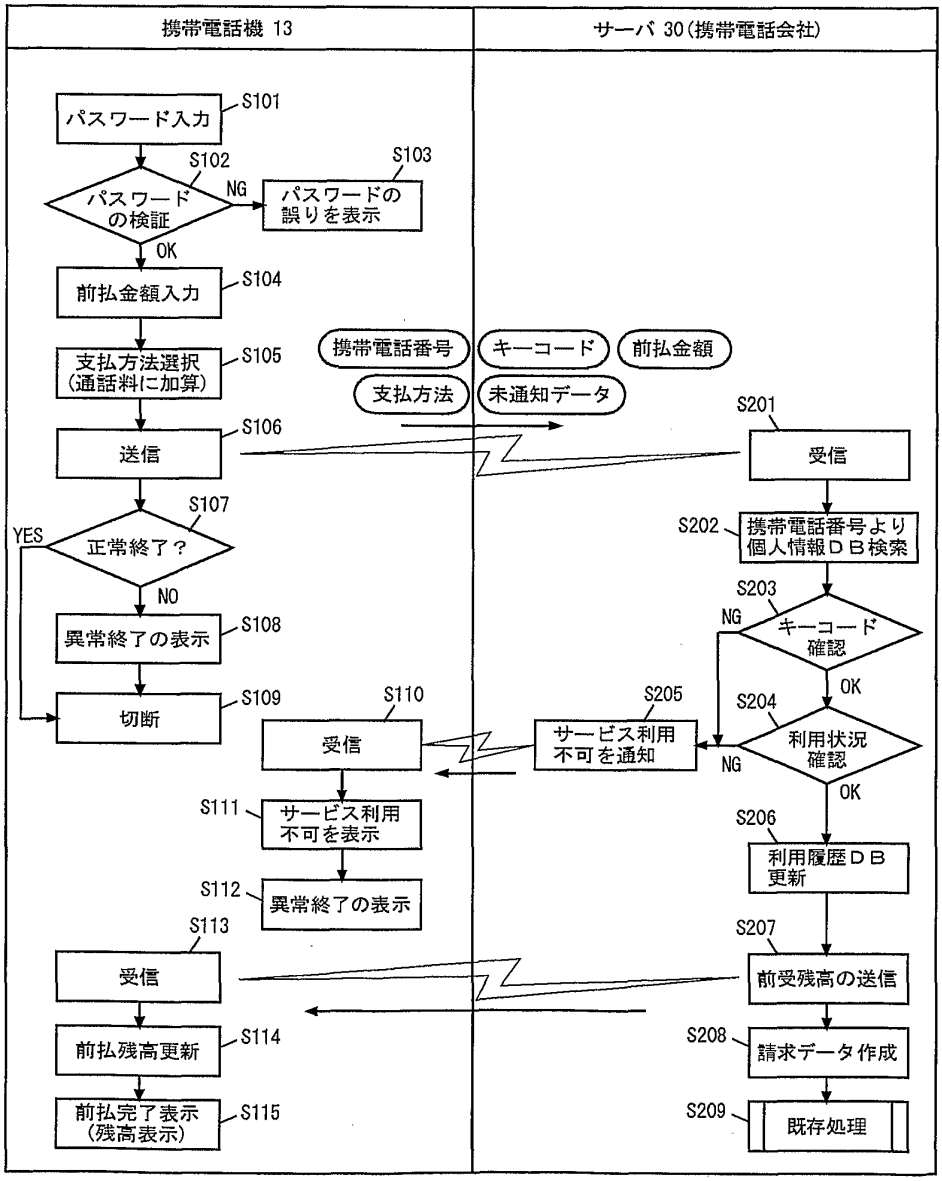

携帯電話機 13
サーバ 30(携帯電話会社)
パスワード入力
S101
S102
パスワードの検証
NG
S103
パスワードの誤りを表示
OK
前払金額入力
S104
支払方法選択(通話料に加算)
S105
携帯電話番号
キーコード
前払金額
支払方法
未通知データ
送信
S106
S201
受信
S107
YES
正常終了?
S202
携帯電話番号より個人情報DB検索
NO
異常終了の表示
S108
S203
NG
キーコード確認
OK
切断
S109
S110
S205
S204
受信
サービス利用不可を通知
利用状況確認
NG
OK
S111
サービス利用不可を表示
S206
利用履歴DB更新
S112
異常終了の表示
S113
S207
受信
前受残高の送信
前払残高更新
S114
S208
請求データ作成
前払完了表示(残高表示)
S115
S209
既存処理

FIG. 9

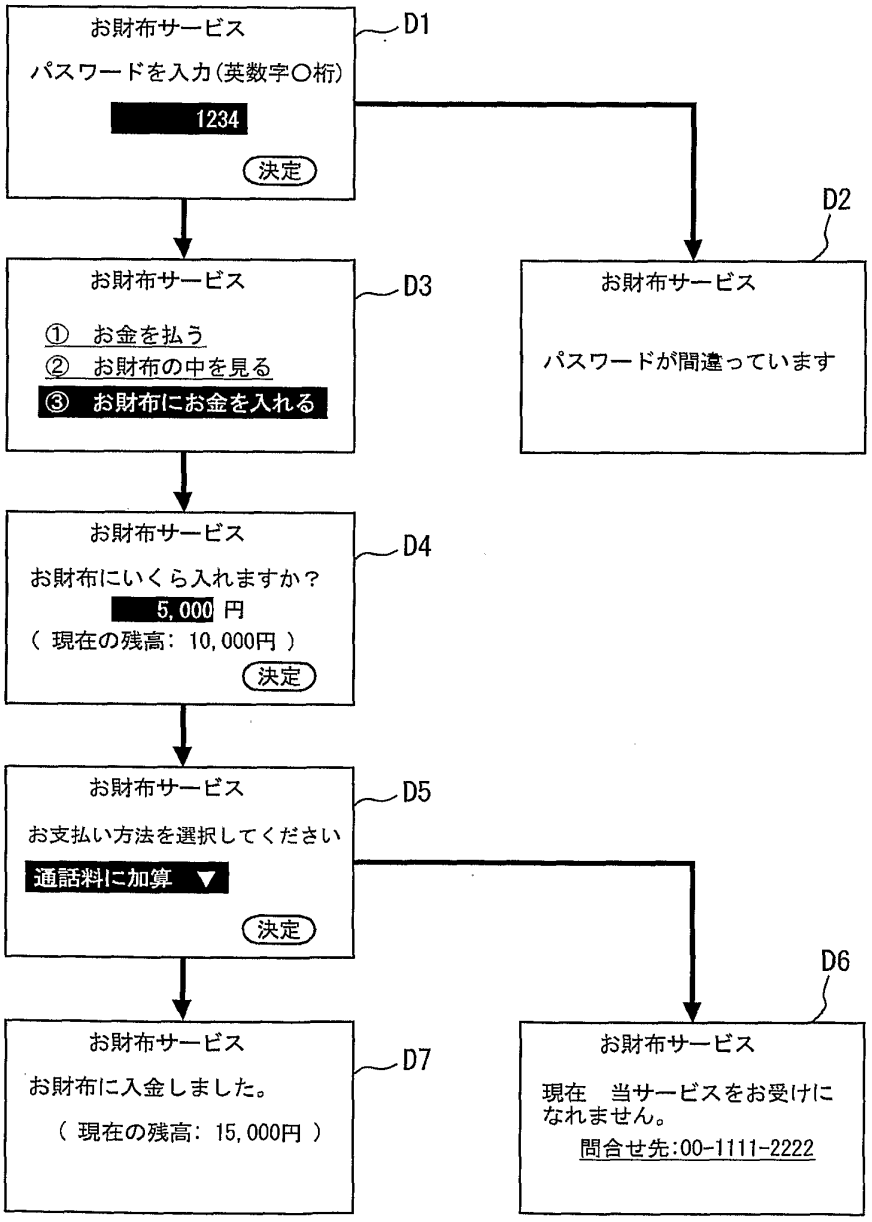

お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D1
D2
お財布サービス
パスワードが間違っています
お財布サービス
① お金を払う
② お財布の中を見る
③ お財布にお金を入れる
D3
お財布サービス
お財布にいくら入れますか？
5,000 円
(現在の残高: 10,000円)
決定
D4
お財布サービス
お支払い方法を選択してください
通話料に加算
決定
D5
D6
お財布サービス
現在 当サービスをお受けになれません。
問合せ先:00-1111-2222
お財布サービス
お財布に入金しました。
(現在の残高: 15,000円)
D7

FIG. 10

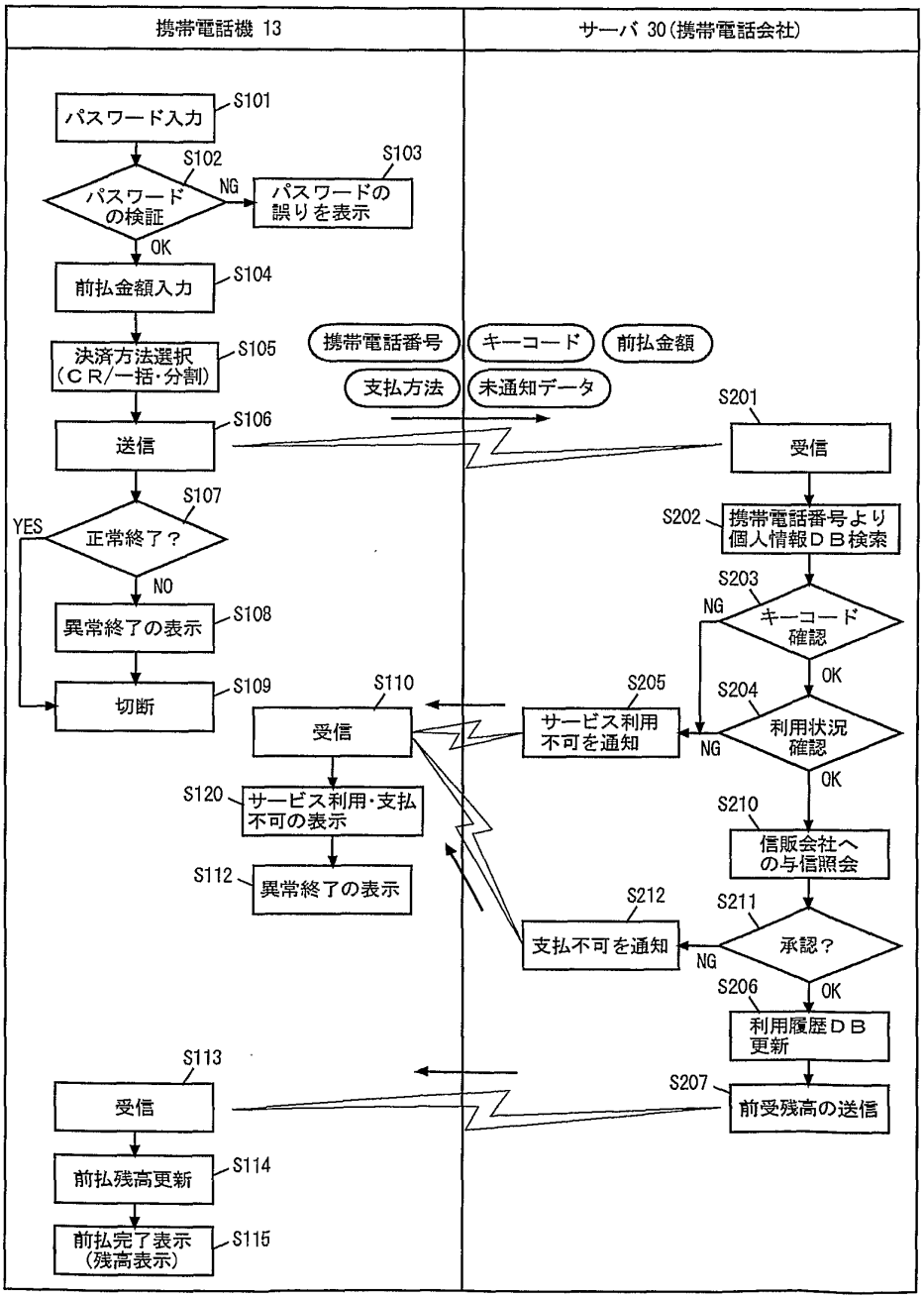

携帯電話機 13
サーバ 30(携帯電話会社)
パスワード入力
S101
S102
パスワードの検証
NG
S103
パスワードの誤りを表示
OK
前払金額入力
S104
決済方法選択(CR/一括・分割)
S105
携帯電話番号
キーコード
前払金額
支払方法
未通知データ
送信
S106
S201
受信
S107
YES
正常終了?
S202
携帯電話番号より個人情報DB検索
NO
S203
NG
キーコード確認
異常終了の表示
S108
OK
S204
利用状況確認
切断
S109
S110
S205
受信
サービス利用不可を通知
NG
OK
S120
サービス利用・支払不可の表示
S210
信販会社への与信照会
S112
異常終了の表示
S212
S211
支払不可を通知
承認?
NG
S206
OK
利用履歴DB更新
S113
S207
受信
前受残高の送信
前払残高更新
S114
前払完了表示(残高表示)
S115

FIG. 11

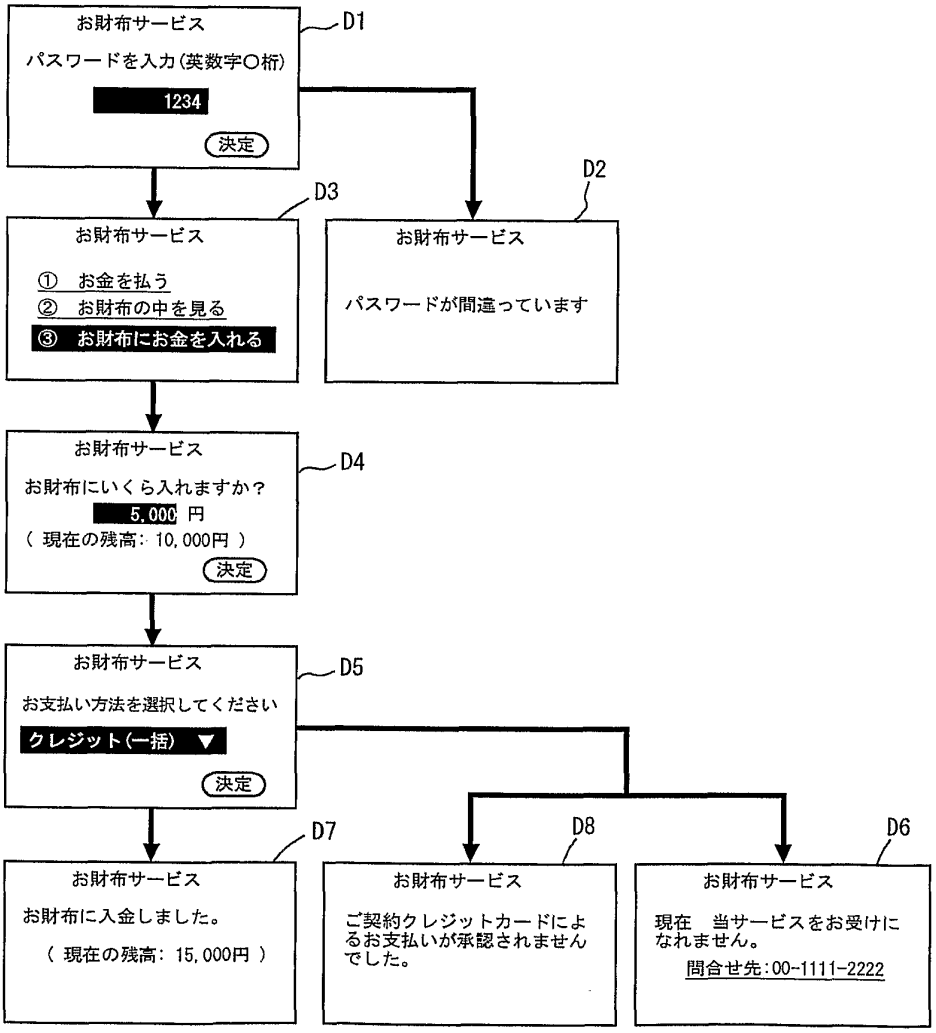

お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D1
D2
D3
お財布サービス
① お金を払う
② お財布の中を見る
③ お財布にお金を入れる
お財布サービス
パスワードが間違っています
お財布サービス
お財布にいくら入れますか？
5,000 円
(現在の残高: 10,000円)
決定
D4
お財布サービス
お支払い方法を選択してください
クレジット(一括) ▼
決定
D5
D7
D8
D6
お財布サービス
お財布に入金しました。
(現在の残高: 15,000円)
お財布サービス
ご契約クレジットカードによるお支払いが承認されませんでした。
お財布サービス
現在 当サービスをお受けになれません。
問合せ先:00-1111-2222

FIG. 12

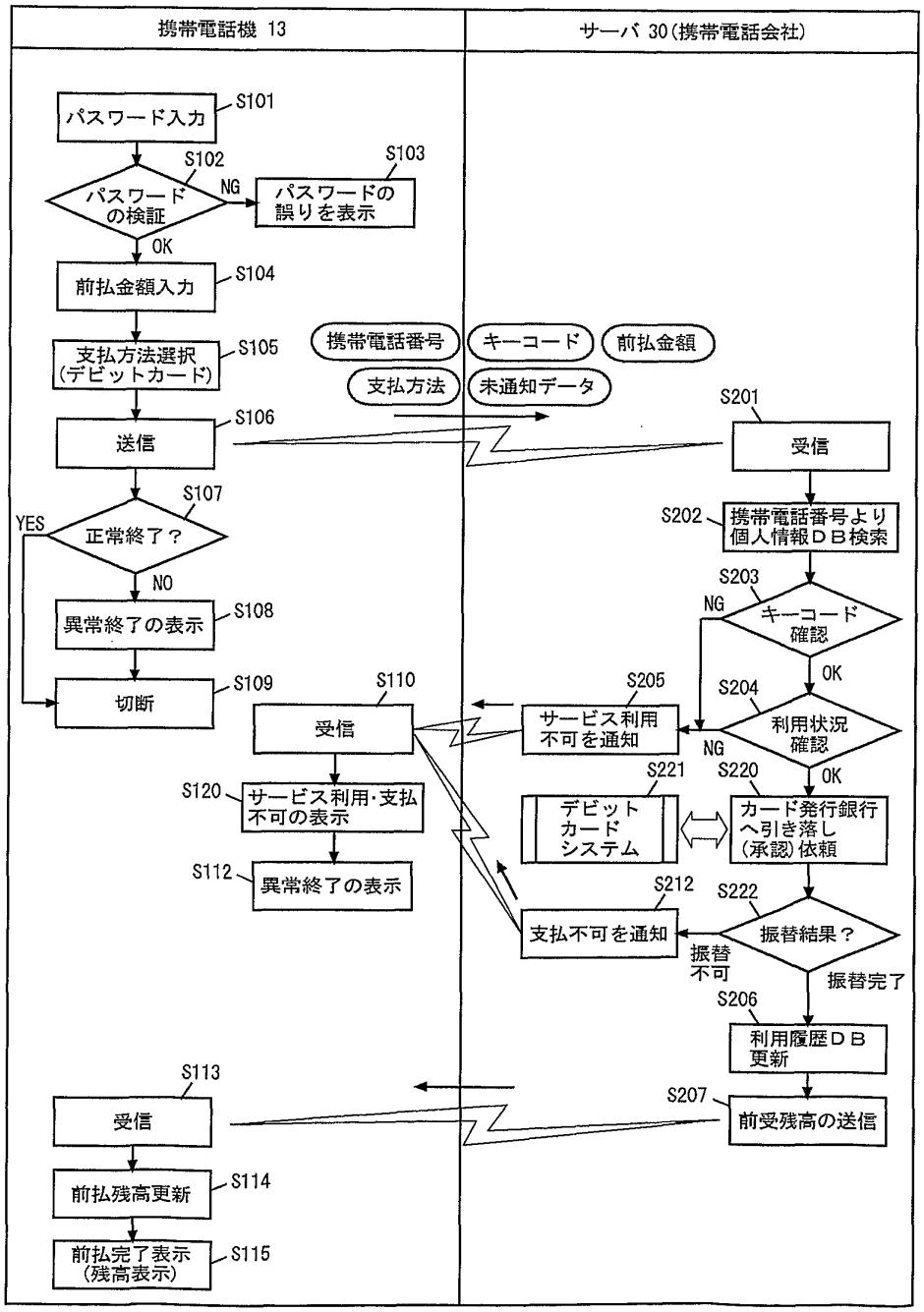

携帯電話機 13
サーバ 30(携帯電話会社)
パスワード入力
S101
S102
パスワードの検証
NG
S103
パスワードの誤りを表示
OK
前払金額入力
S104
支払方法選択(デビットカード)
S105
携帯電話番号
キーコード
前払金額
支払方法
未通知データ
送信
S106
S201
受信
S107
YES
正常終了？
S202
携帯電話番号より個人情報ＤＢ検索
NO
異常終了の表示
S108
S203
NG
キーコード確認
OK
切断
S109
S110
S205
S204
受信
サービス利用不可を通知
利用状況確認
NG
S221
S220
OK
S120
サービス利用・支払不可の表示
デビットカードシステム
カード発行銀行へ引き落し(承認)依頼
S112
異常終了の表示
S212
S222
支払不可を通知
振替結果？
振替不可
振替完了
S206
利用履歴ＤＢ更新
S113
S207
受信
前受残高の送信
前払残高更新
S114
前払完了表示(残高表示)
S115

FIG. 13

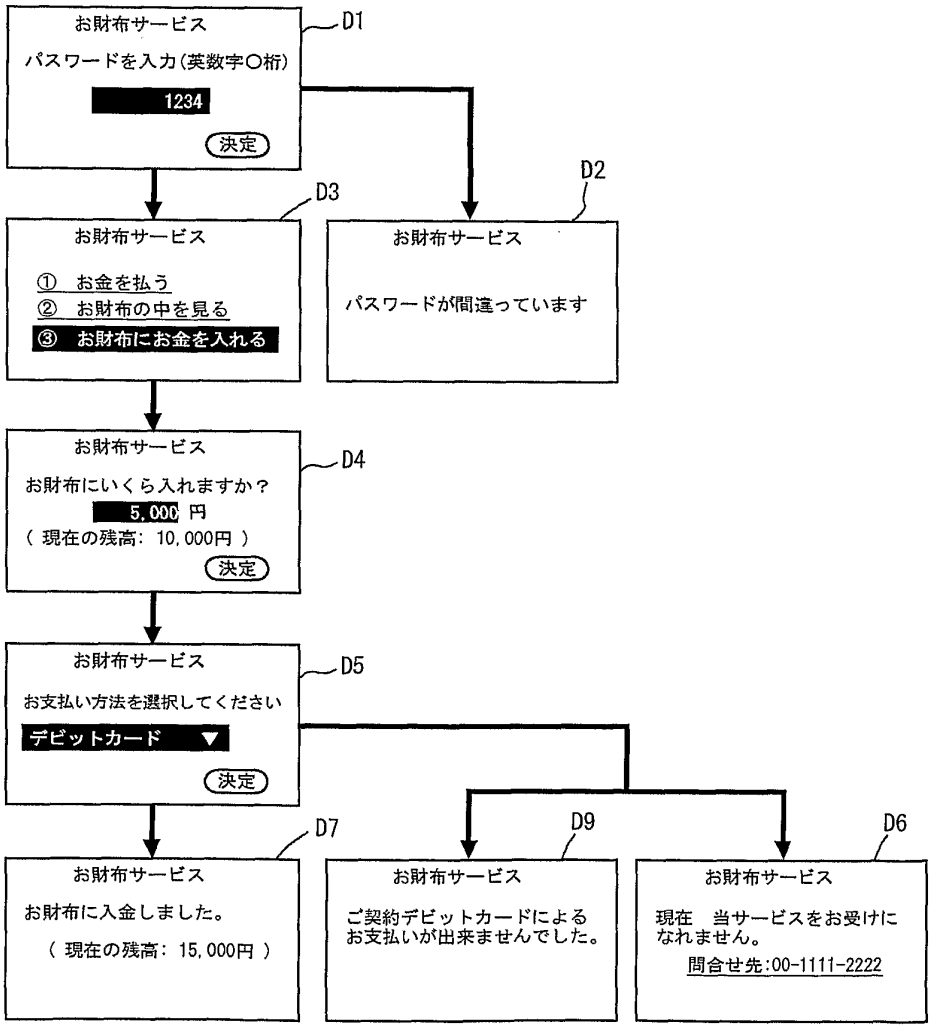

お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D1
D2
D3
お財布サービス
① お金を払う
② お財布の中を見る
③ お財布にお金を入れる
お財布サービス
パスワードが間違っています
お財布サービス
お財布にいくら入れますか？
5,000 円
(現在の残高: 10,000円)
決定
D4
お財布サービス
お支払い方法を選択してください
デビットカード
決定
D5
D7
D9
D6
お財布サービス
お財布に入金しました。
(現在の残高: 15,000円)
お財布サービス
ご契約デビットカードによる
お支払いが出来ませんでした。
お財布サービス
現在 当サービスをお受けに
なれません。
問合せ先:00-1111-2222

FIG. 14

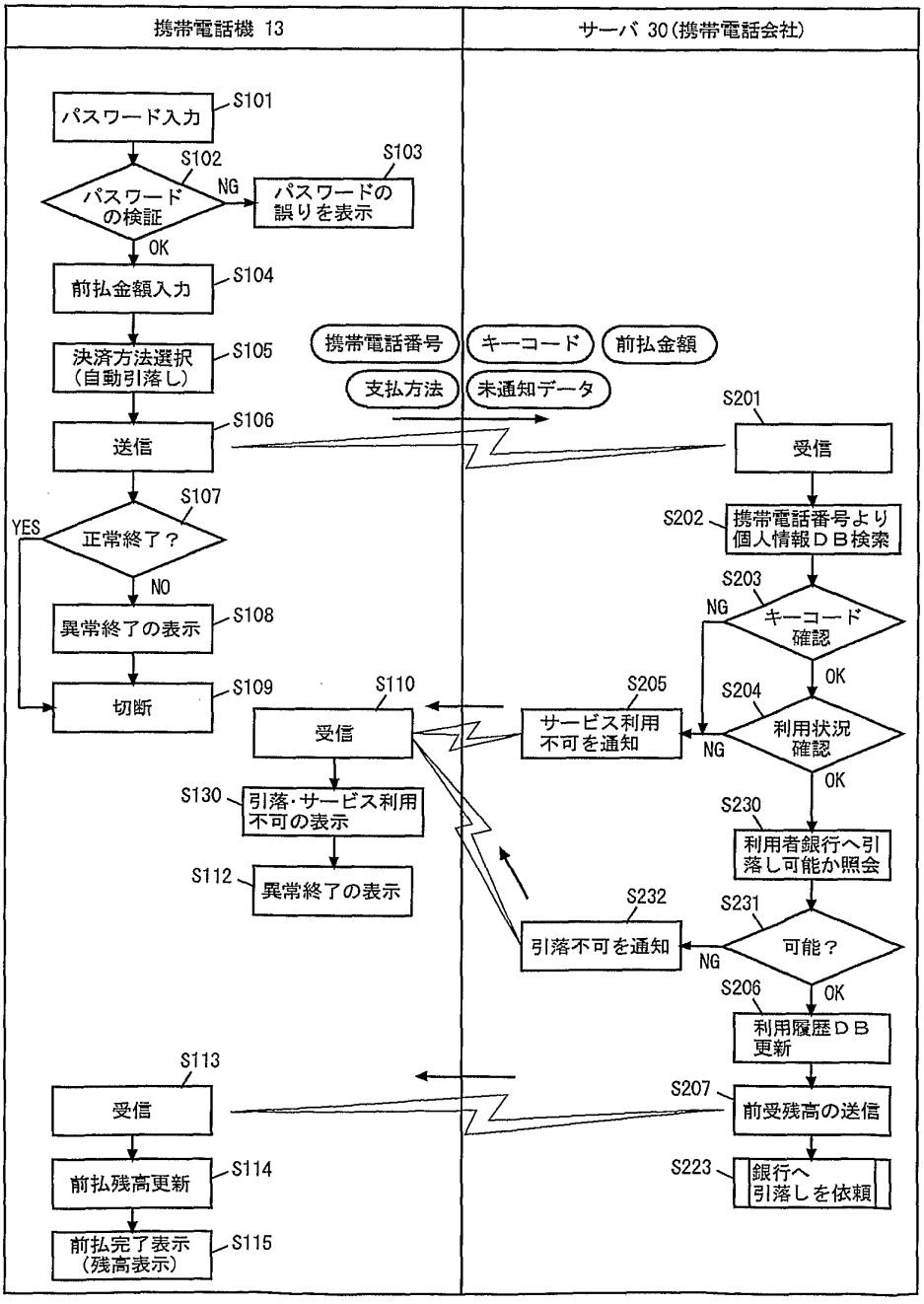

携帯電話機 13
サーバ 30(携帯電話会社)
パスワード入力
S101
S102
パスワードの検証
NG
S103
パスワードの誤りを表示
OK
前払金額入力
S104
決済方法選択(自動引落し)
S105
携帯電話番号
キーコード
前払金額
支払方法
未通知データ
送信
S106
S201
受信
S107
YES
正常終了？
S202
携帯電話番号より個人情報ＤＢ検索
NO
異常終了の表示
S108
S203
NG
キーコード確認
OK
切断
S109
S110
S205
S204
受信
サービス利用不可を通知
利用状況確認
NG
OK
S130
引落・サービス利用不可の表示
S230
利用者銀行へ引落し可能か照会
S112
異常終了の表示
S232
S231
引落不可を通知
可能？
NG
S206
OK
利用履歴ＤＢ更新
S113
受信
S207
前受残高の送信
前払残高更新
S114
S223
銀行へ引落しを依頼
前払完了表示(残高表示)
S115

FIG. 15

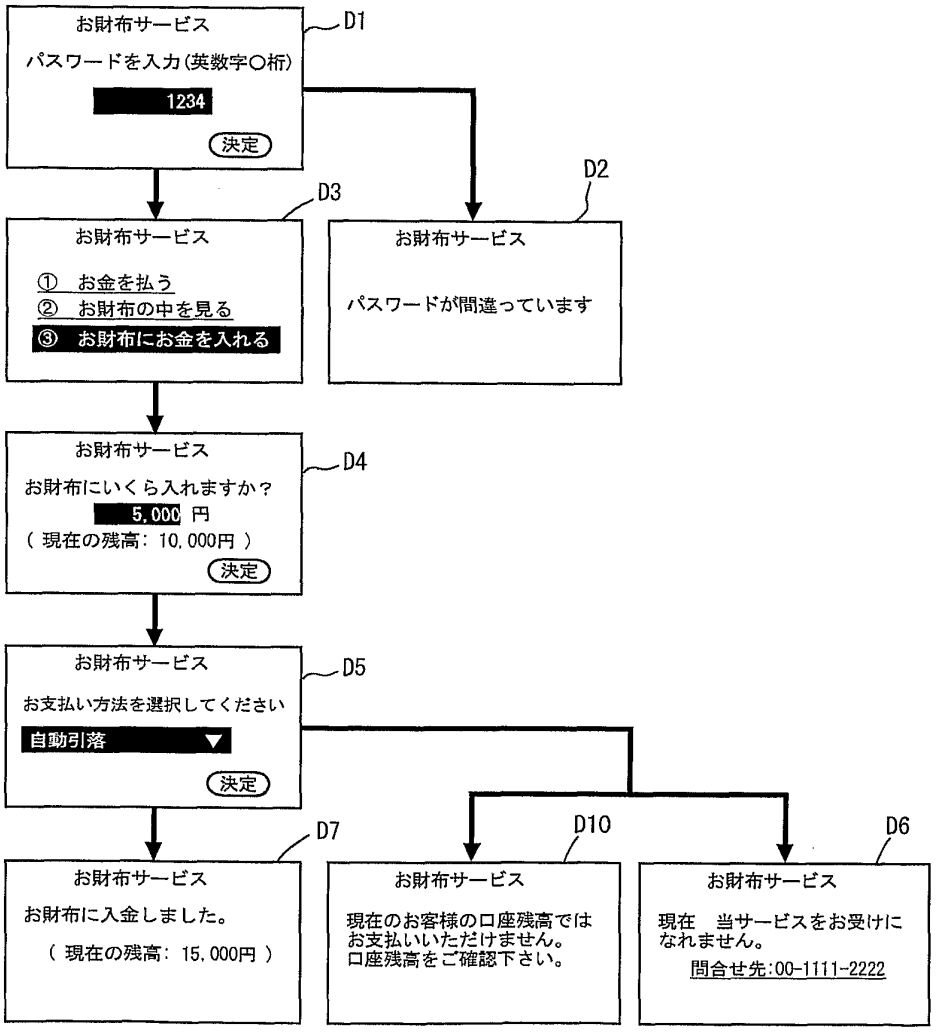

お財布サービス
パスワードを入力(英数字〇桁)
1234
決定
D1
D2
D3
お財布サービス
① お金を払う
② お財布の中を見る
③ お財布にお金を入れる
お財布サービス
パスワードが間違っています
お財布サービス
お財布にいくら入れますか？
5,000 円
(現在の残高: 10,000円)
決定
D4
お財布サービス
お支払い方法を選択してください
自動引落
決定
D5
D7
D10
D6
お財布サービス
お財布に入金しました。
(現在の残高: 15,000円)
お財布サービス
現在のお客様の口座残高では
お支払いいただけません。
口座残高をご確認下さい。
お財布サービス
現在 当サービスをお受けに
なれません。
問合せ先:00-1111-2222

FIG. 16

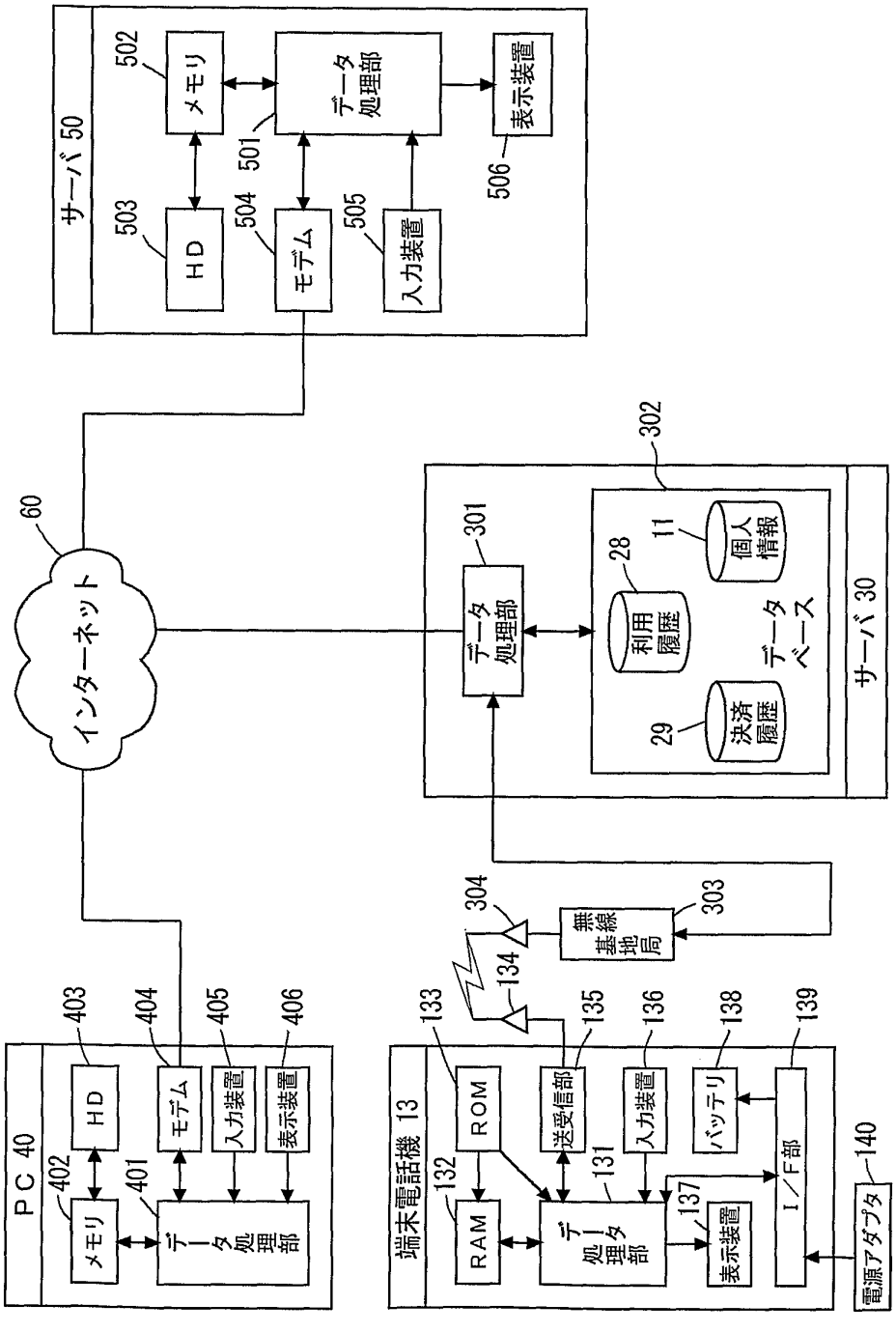

サーバ 50
メモリ
502
データ処理部
501
表示装置
506
HD
503
モデム
504
入力装置
505
インターネット
60
データ処理部
301
302
個人情報
11
利用履歴
28
決済履歴
29
データベース
サーバ 30
無線基地局
303
304
134
PC 40
メモリ
402
HD
403
モデム
404
入力装置
405
表示装置
406
データ処理部
401
端末電話機 13
RAM
132
ROM
133
送受信部
135
入力装置
136
バッテリ
138
I／F部
139
電源アダプタ
140
データ処理部
131
表示装置
137

FIG. 17

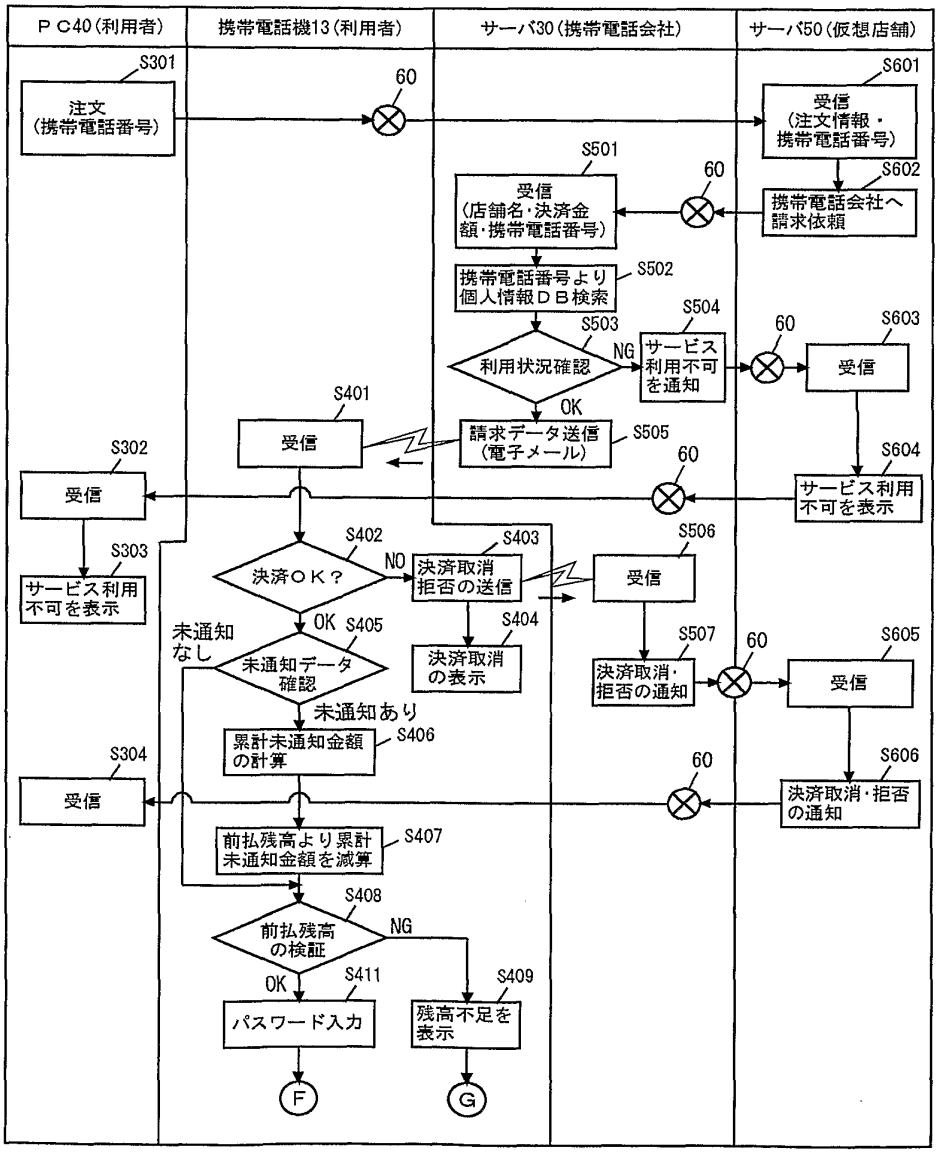
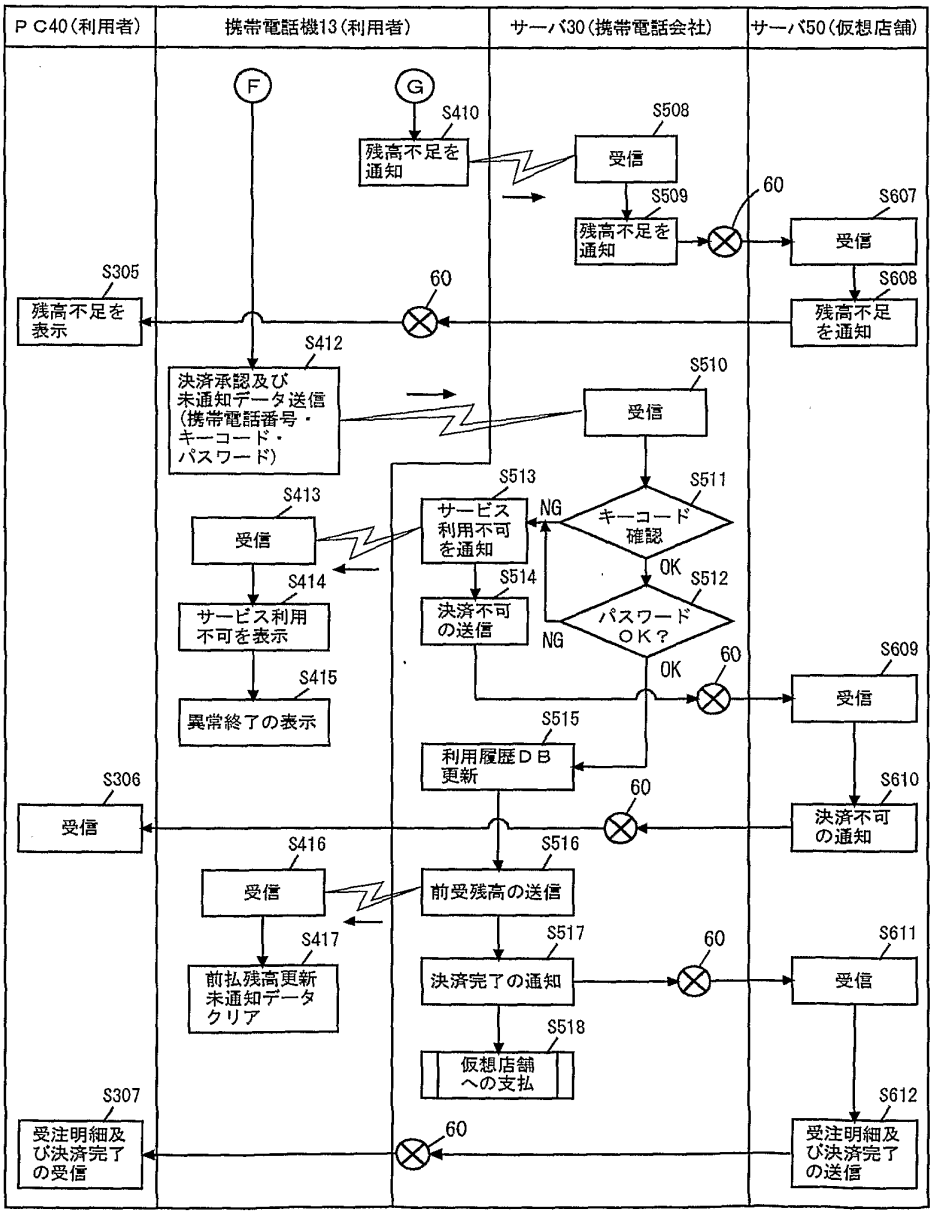

PC40(利用者)
携帯電話機13(利用者)
サーバ30(携帯電話会社)
サーバ50(仮想店舗)
S301
注文
(携帯電話番号)
60
S601
受信
(注文情報・
携帯電話番号)
S501
受信
(店舗名・決済金
額・携帯電話番号)
60
S602
携帯電話会社へ
請求依頼
携帯電話番号より
個人情報DB検索
S502
S503
利用状況確認
NG
S504
サービス
利用不可
を通知
60
S603
受信
OK
S401
受信
請求データ送信
(電子メール)
S505
60
S604
サービス利用
不可を表示
S302
受信
S303
サービス利用
不可を表示
S402
決済OK?
NO
S403
決済取消
拒否の送信
S506
受信
未通知
なし
OK
S405
未通知データ
確認
S404
決済取消
の表示
S507
決済取消・
拒否の通知
60
S605
受信
未通知あり
累計未通知金額
の計算
S406
S304
受信
60
S606
決済取消・拒否
の通知
前払残高より累計
未通知金額を減算
S407
S408
前払残高
の検証
NG
OK
S411
パスワード入力
S409
残高不足を
表示
F
G

FIG. 18



APPL-1002
APPLE INC. / Page 746 of 1892

FIG. 19

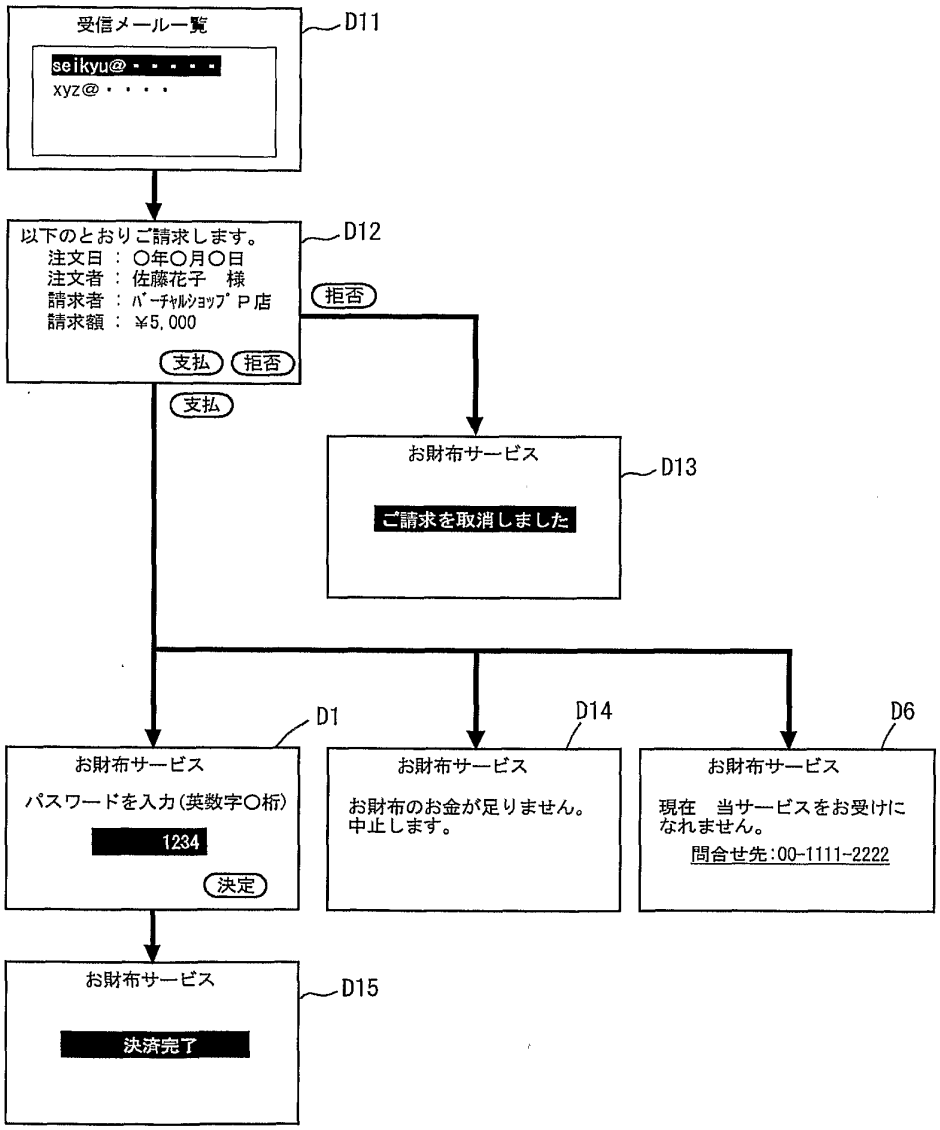

受信メール一覧
D11
seikyu@・・・・・
xyz@・・・・
以下のとおりご請求します。
注文日 ： ○年○月○日
注文者 ： 佐藤花子 様
請求者 ： ﾊﾞｰﾁｬﾙｼｮｯﾌﾟP店
請求額 ： ¥5,000
D12
支払
拒否
拒否
支払
お財布サービス
ご請求を取消しました
D13
お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D1
お財布サービス
お財布のお金が足りません。
中止します。
D14
お財布サービス
現在 当サービスをお受けになれません。
問合せ先:00-1111-2222
D6
お財布サービス
決済完了
D15

FIG. 20

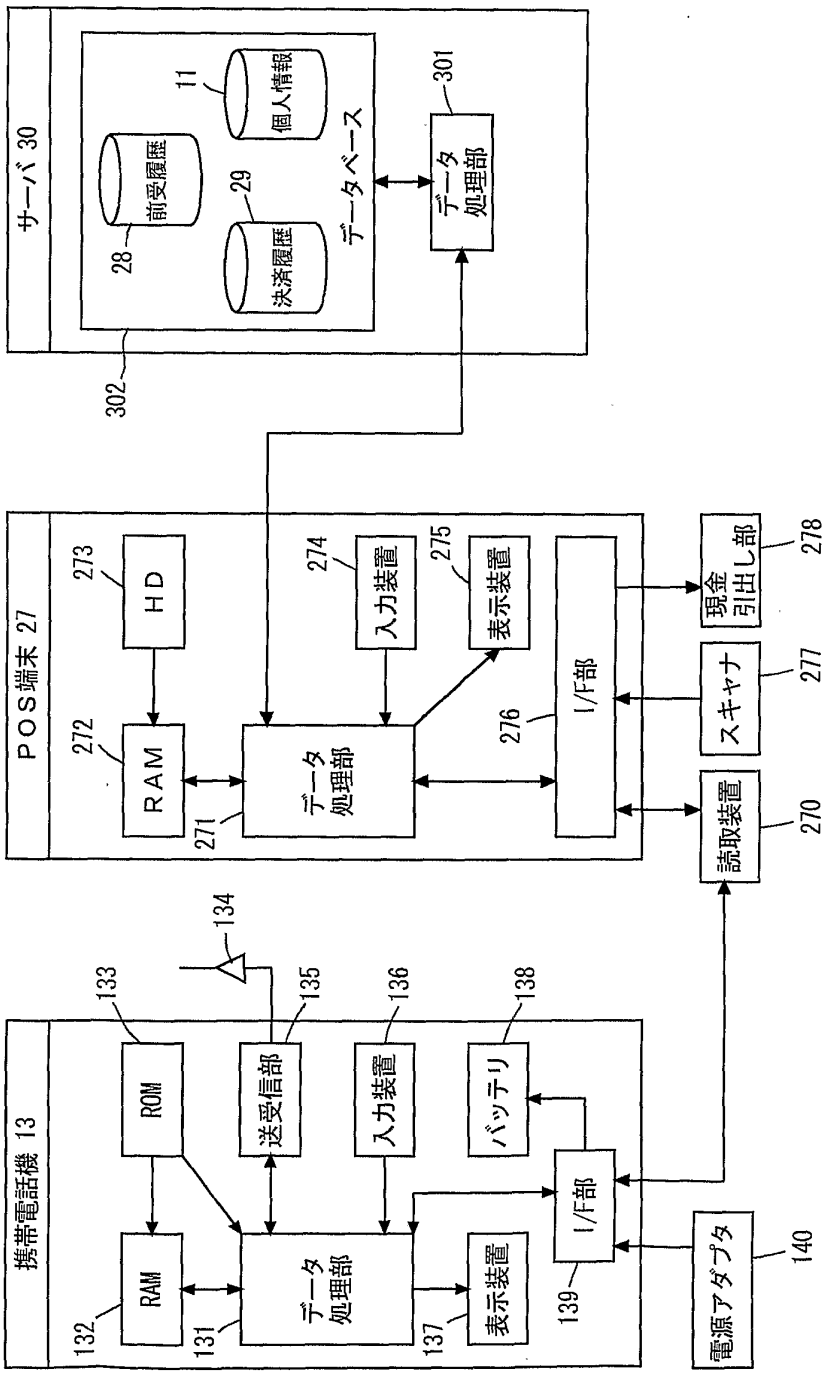

携帯電話機 13
ROM
RAM
データ処理部
送受信部
入力装置
バッテリ
表示装置
I/F部
電源アダプタ
POS端末 27
HD
RAM
データ処理部
入力装置
表示装置
I/F部
読取装置
スキャナ
現金引出し部
サーバ 30
データベース
前受履歴
決済履歴
個人情報
データ処理部
131
132
133
134
135
136
137
138
139
140
271
272
273
274
275
276
277
278
28
29
301
302

FIG. 21

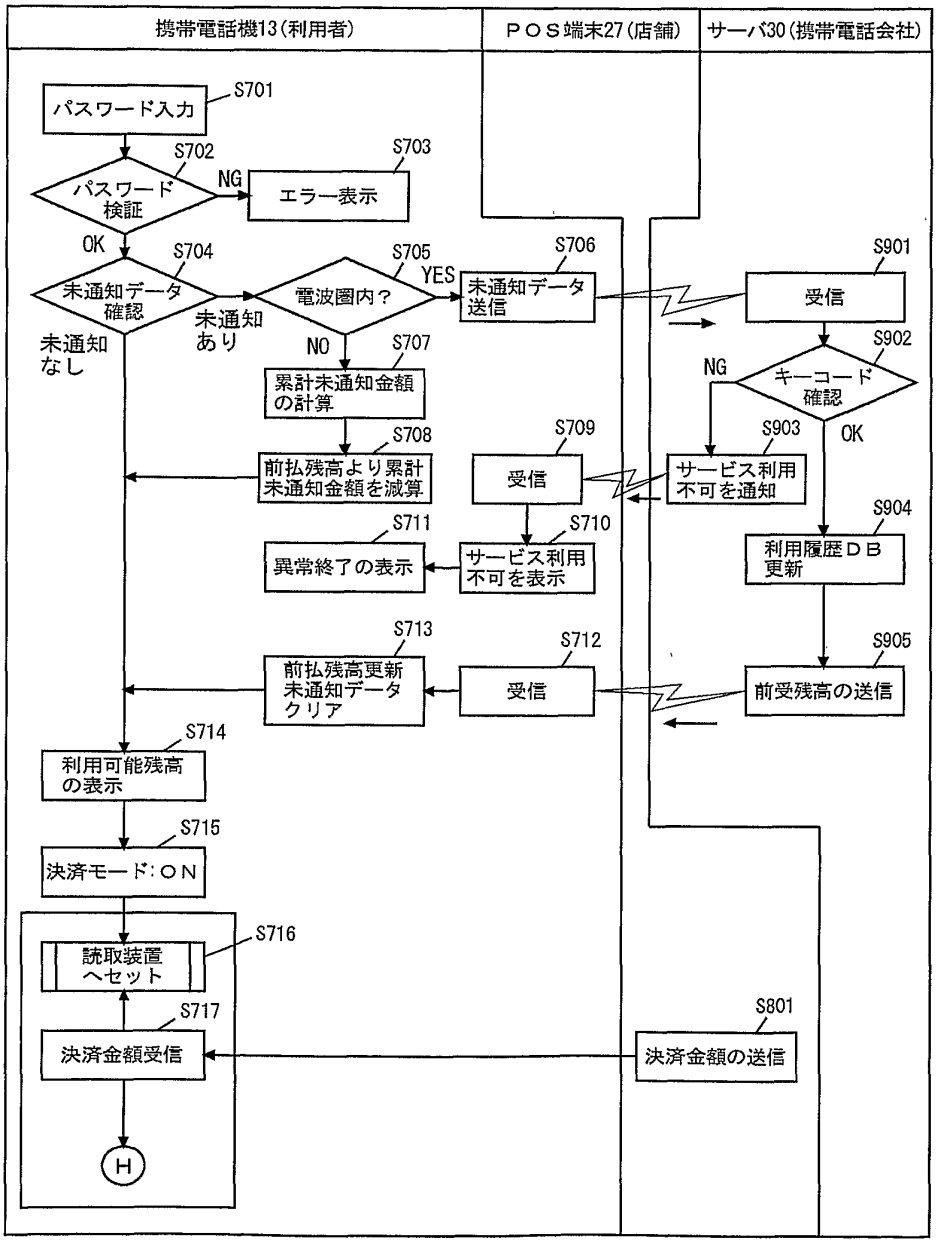
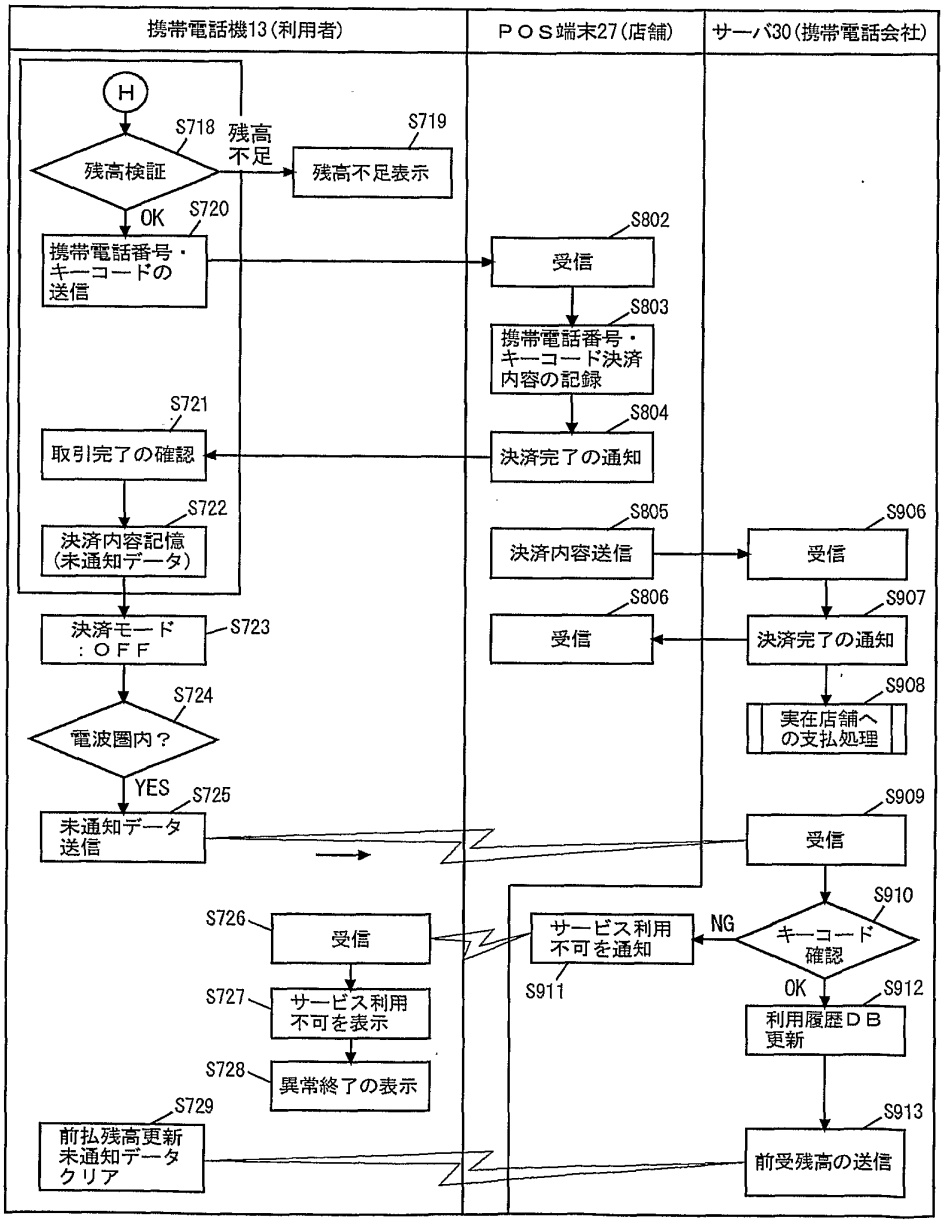

携帯電話機13(利用者)
POS端末27(店舗)
サーバ30(携帯電話会社)
パスワード入力
S701
パスワード検証
S702
NG
エラー表示
S703
OK
未通知データ確認
S704
未通知なし
未通知あり
電波圏内?
S705
YES
NO
未通知データ送信
S706
受信
S901
キーコード確認
S902
NG
OK
累計未通知金額の計算
S707
前払残高より累計未通知金額を減算
S708
受信
S709
サービス利用不可を通知
S903
利用履歴DB更新
S904
異常終了の表示
S711
サービス利用不可を表示
S710
前払残高更新未通知データクリア
S713
受信
S712
前受残高の送信
S905
利用可能残高の表示
S714
決済モード:ON
S715
読取装置へセット
S716
決済金額受信
S717
決済金額の送信
S801
H

FIG. 22



APPL-1002
APPLE INC. / Page 750 of 1892

FIG. 23

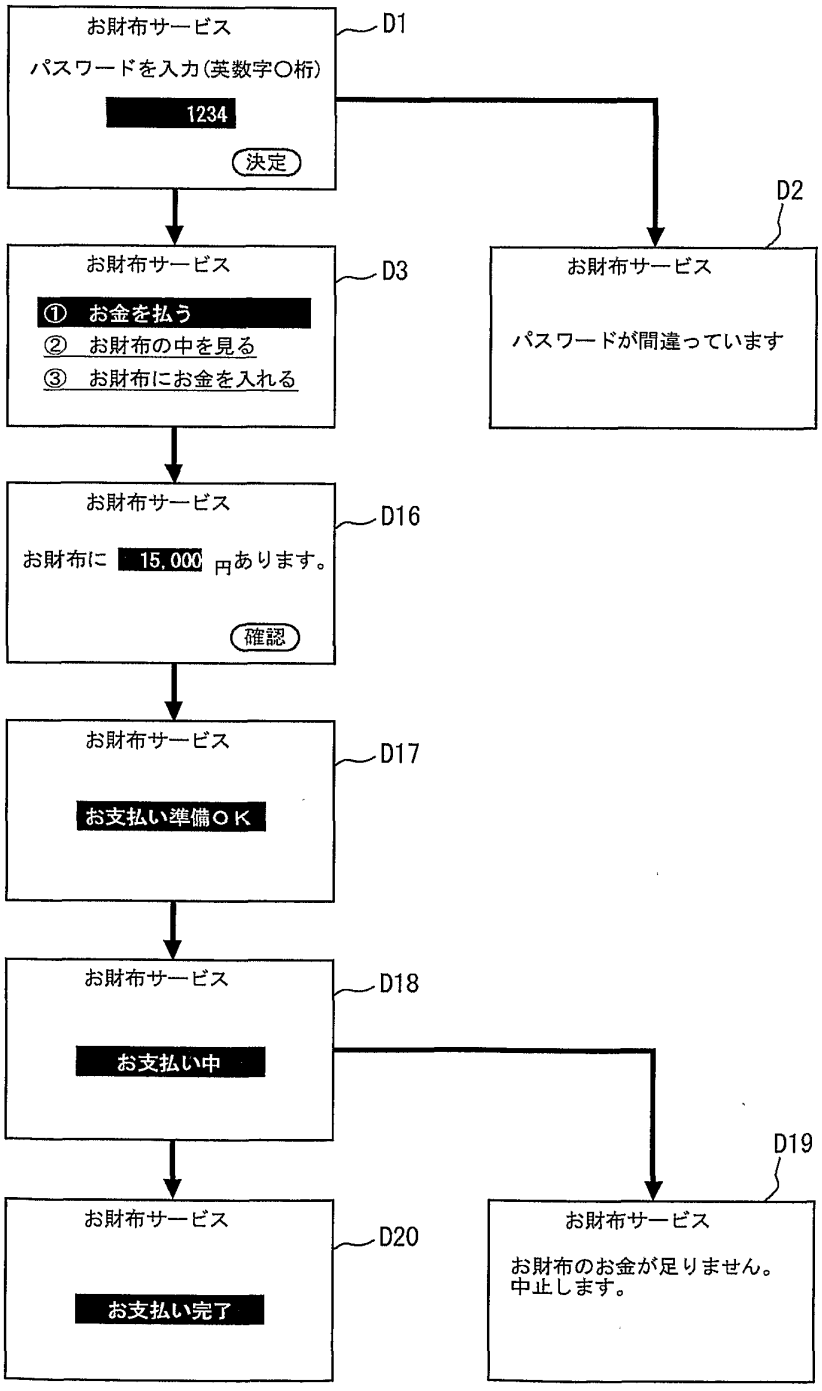
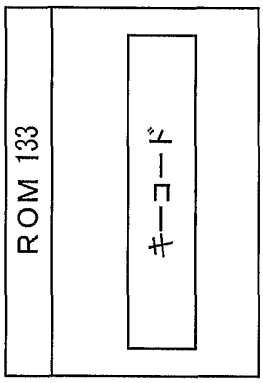
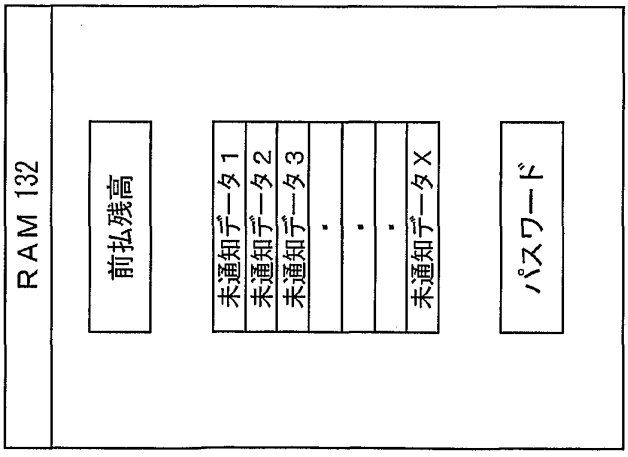

お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D1
D2
お財布サービス
パスワードが間違っています
お財布サービス
① お金を払う
② お財布の中を見る
③ お財布にお金を入れる
D3
お財布サービス
お財布に 15,000 円あります。
確認
D16
お財布サービス
お支払い準備○K
D17
お財布サービス
お支払い中
D18
D19
お財布サービス
お財布のお金が足りません。
中止します。
お財布サービス
お支払い完了
D20

FIG. 24





APPL-1002
APPLE INC. / Page 752 of 1892

FIG. 25

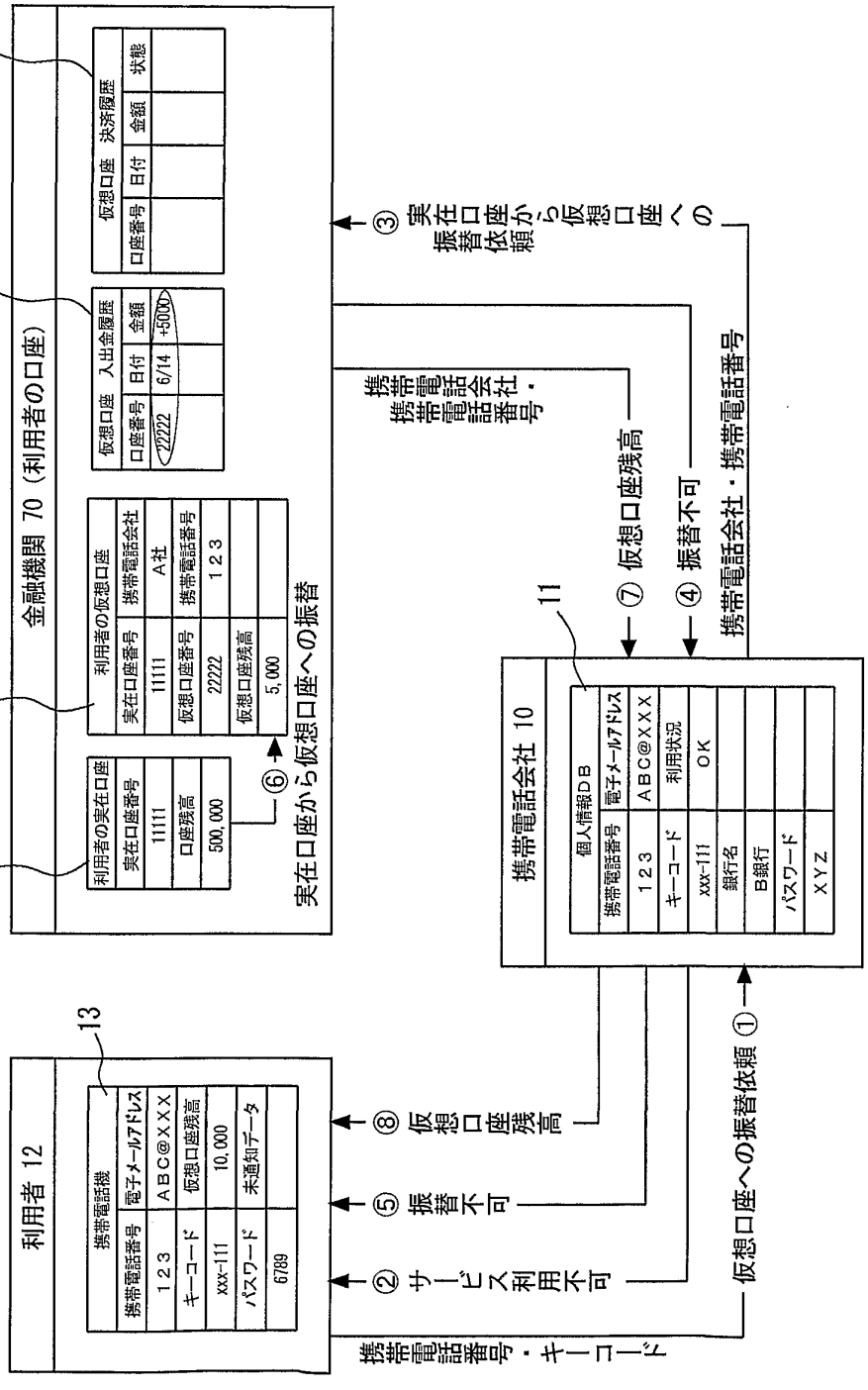

利用者 12
13
携帯電話機
携帯電話番号
123
電子メールアドレス
ABC@XXX
キーコード
xxx-111
仮想口座残高
10,000
パスワード
6789
未通知データ
金融機関 70（利用者の口座）
710
利用者の実在口座
実在口座番号
11111
口座残高
500,000
110
利用者の仮想口座
実在口座番号
11111
携帯電話会社
A社
仮想口座番号
22222
携帯電話番号
123
仮想口座残高
5,000
712
仮想口座 入出金履歴
口座番号
日付
金額
22222
6/14
+5000
714
仮想口座 決済履歴
口座番号
日付
金額
状態
携帯電話会社 10
11
個人情報DB
携帯電話番号
電子メールアドレス
123
ABC@XXX
キーコード
利用状況
xxx-111
OK
銀行名
B銀行
パスワード
XYZ
⑥ 実在口座から仮想口座への振替
③ 実在口座から仮想口座への振替依頼
携帯電話会社・携帯電話番号
⑦ 仮想口座残高
④ 振替不可
携帯電話会社・携帯電話番号
仮想口座への振替依頼 ①
携帯電話番号・キーコード
② サービス利用不可
⑤ 振替不可
⑧ 仮想口座残高

FIG. 26

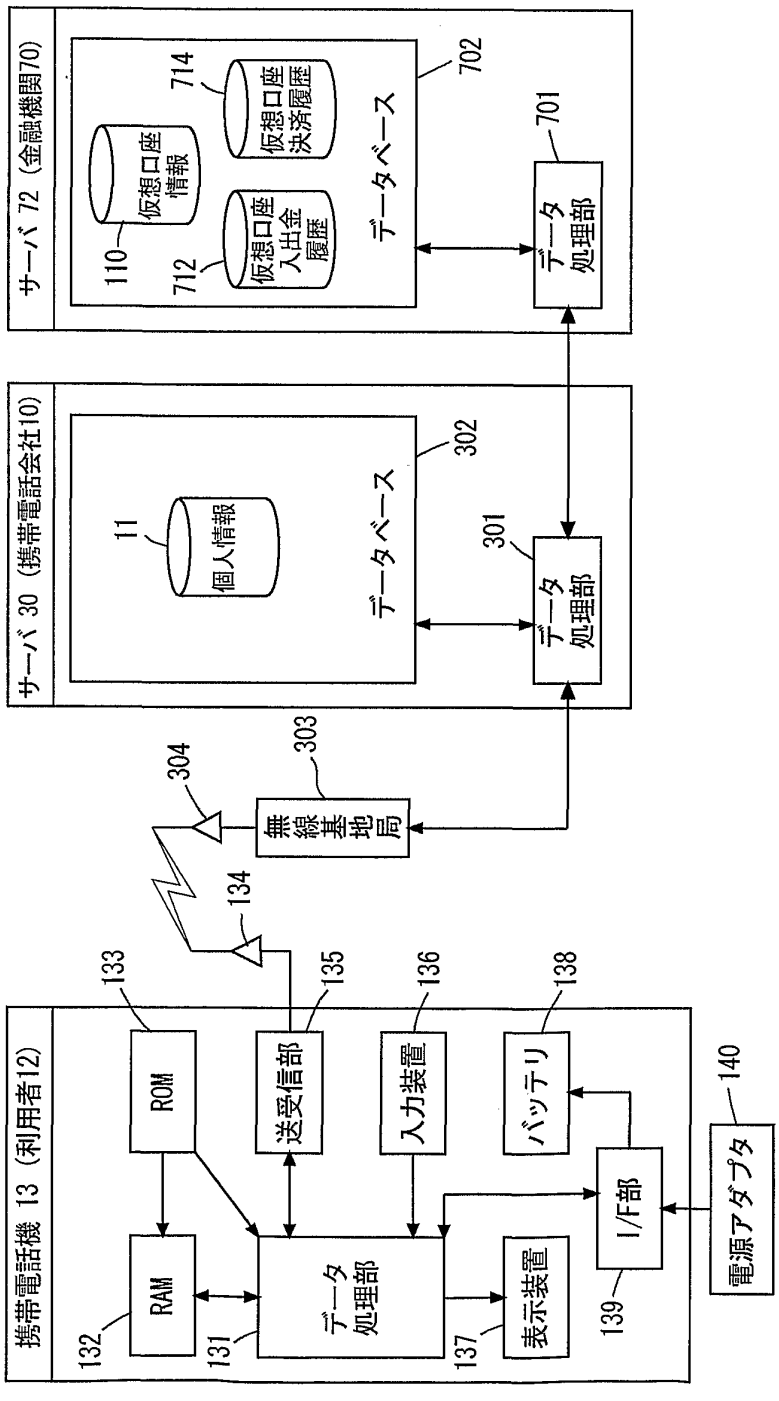

携帯電話機 13（利用者12）
ROM
RAM
データ処理部
送受信部
入力装置
表示装置
バッテリ
I/F部
電源アダプタ
133
132
131
135
136
137
138
139
140
134
304
303
無線基地局
サーバ 30（携帯電話会社10）
11
個人情報
データベース
302
データ処理部
301
サーバ 72（金融機関70）
110
仮想口座情報
712
仮想口座入出金履歴
714
仮想口座決済履歴
データベース
702
データ処理部
701

FIG. 27

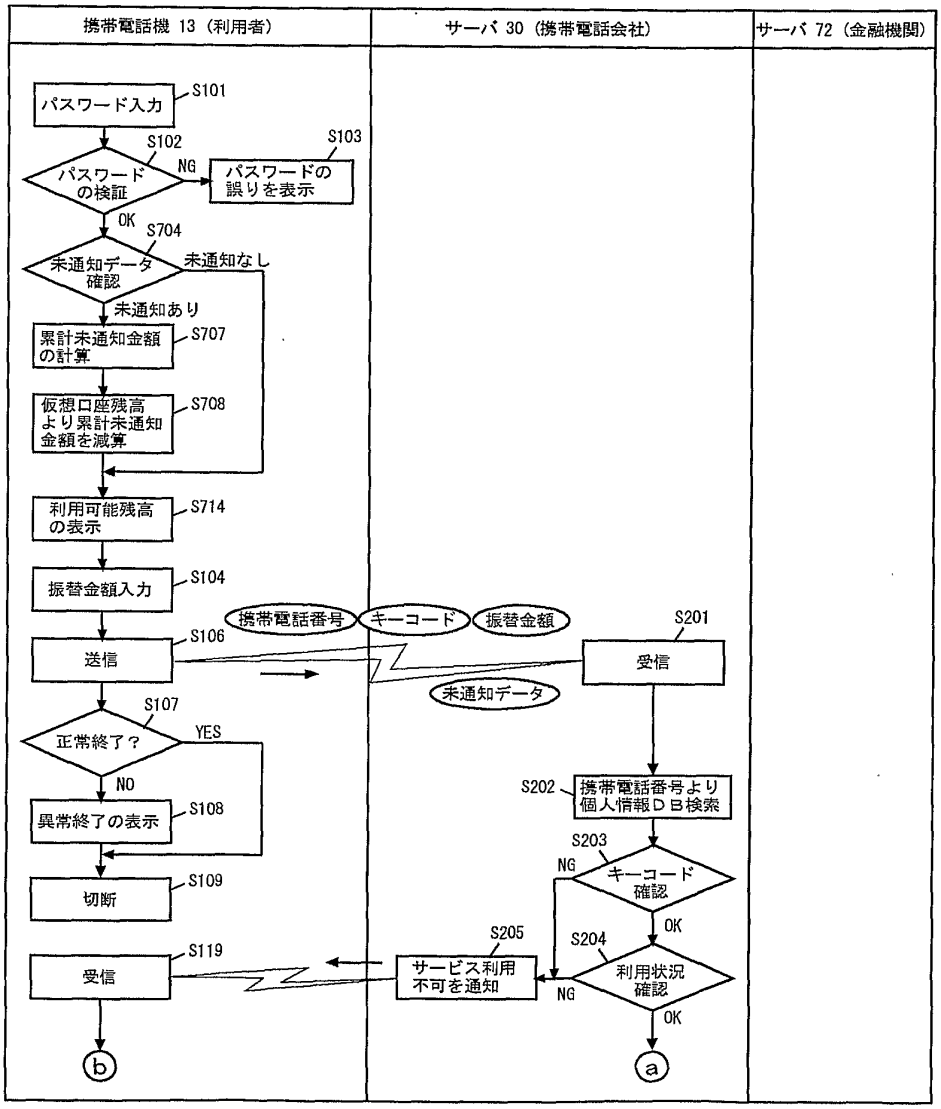

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 72（金融機関）
パスワード入力
S101
S102
パスワードの検証
NG
S103
パスワードの誤りを表示
OK
S704
未通知データ確認
未通知なし
未通知あり
累計未通知金額の計算
S707
仮想口座残高より累計未通知金額を減算
S708
利用可能残高の表示
S714
振替金額入力
S104
携帯電話番号
キーコード
振替金額
S106
送信
S201
受信
未通知データ
S107
正常終了？
YES
NO
異常終了の表示
S108
切断
S109
S202
携帯電話番号より個人情報ＤＢ検索
S203
NG
キーコード確認
OK
S204
利用状況確認
NG
OK
S205
サービス利用不可を通知
S119
受信
b
a

FIG. 28

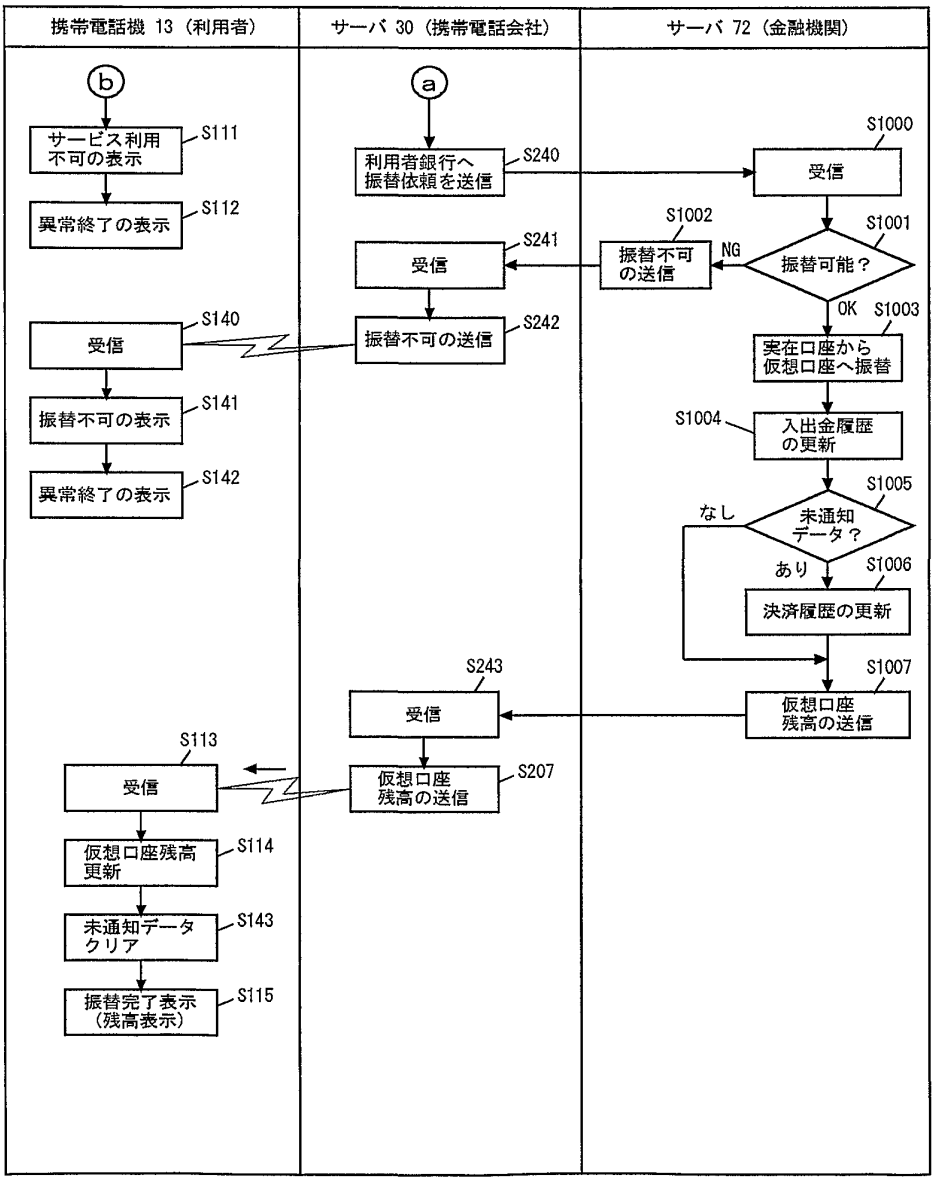
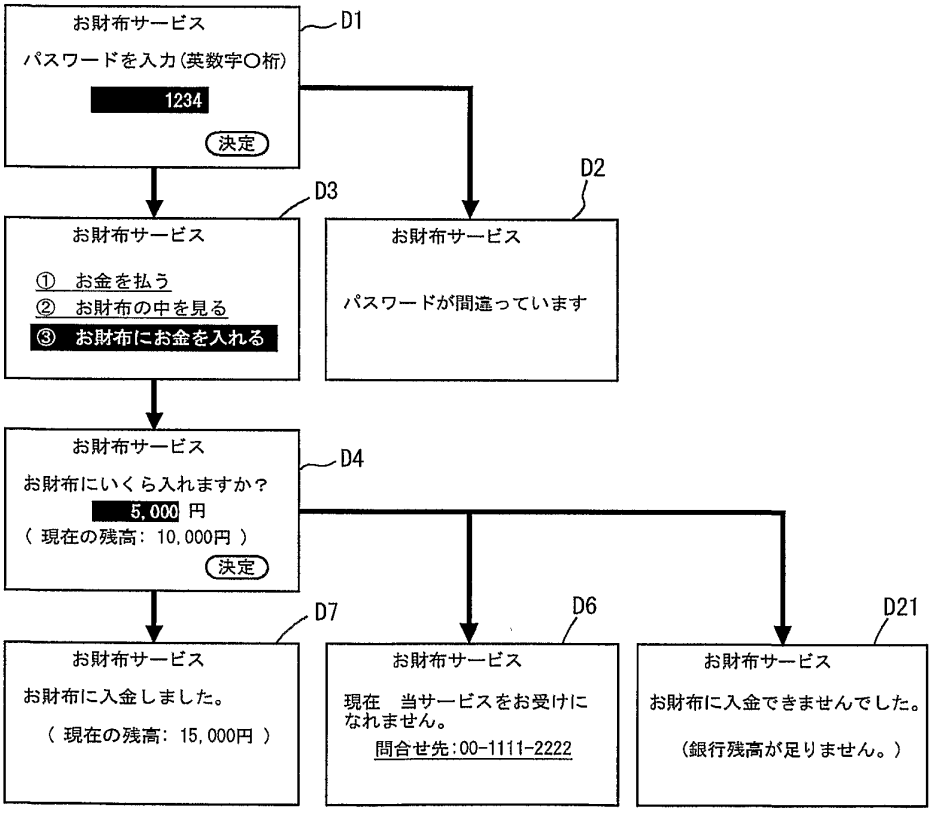
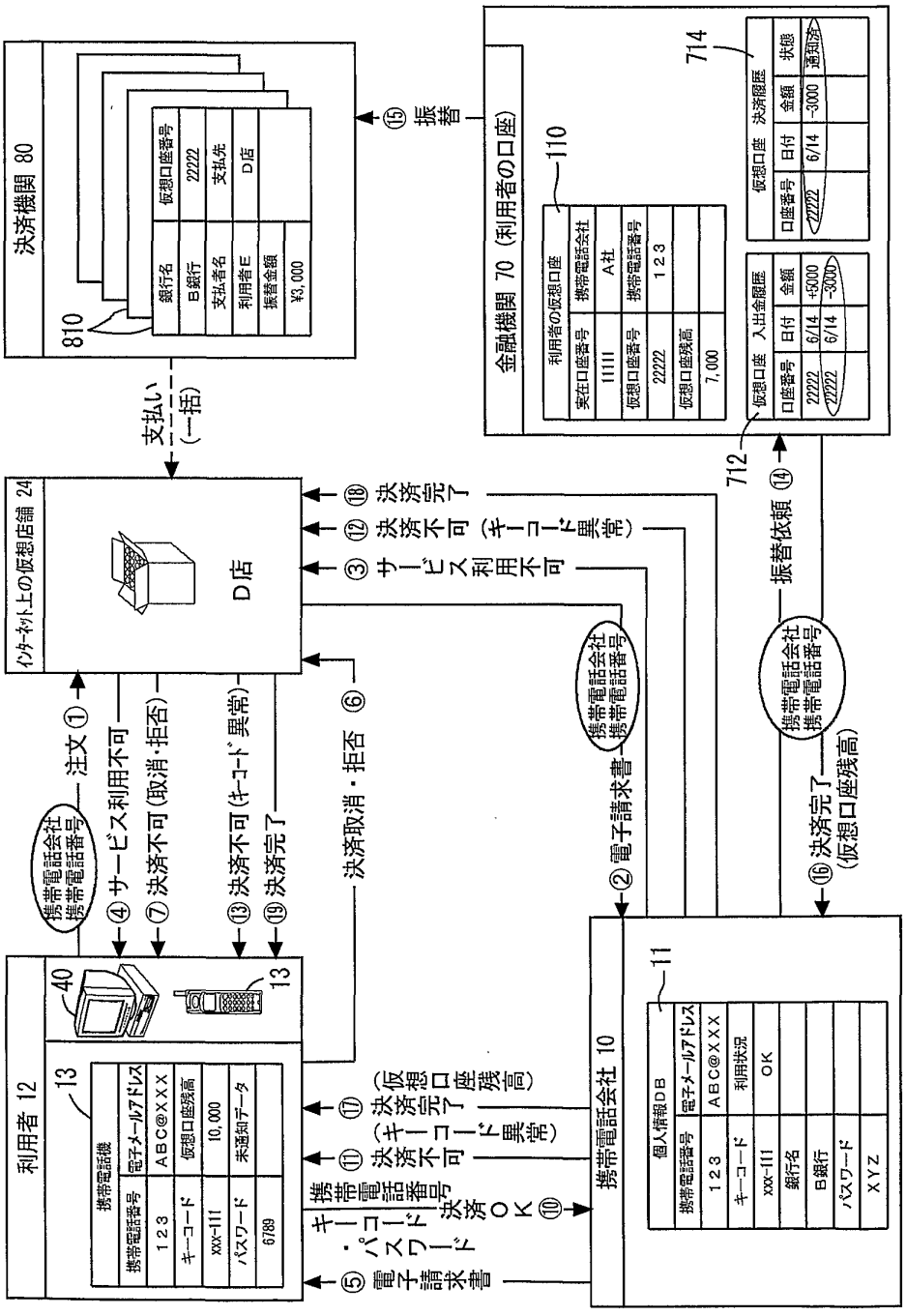

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 72（金融機関）
b
a
サービス利用不可の表示
S111
異常終了の表示
S112
受信
S140
振替不可の表示
S141
異常終了の表示
S142
利用者銀行へ振替依頼を送信
S240
受信
S241
振替不可の送信
S242
受信
S1000
振替不可の送信
S1002
NG
振替可能？
S1001
OK
実在口座から仮想口座へ振替
S1003
入出金履歴の更新
S1004
なし
未通知データ？
S1005
あり
決済履歴の更新
S1006
仮想口座残高の送信
S1007
受信
S243
仮想口座残高の送信
S207
受信
S113
仮想口座残高更新
S114
未通知データクリア
S143
振替完了表示（残高表示）
S115

FIG. 29



APPL-1002
APPLE INC. / Page 757 of 1892

FIG. 30



APPL-1002
APPLE INC. / Page 758 of 1892

FIG. 31

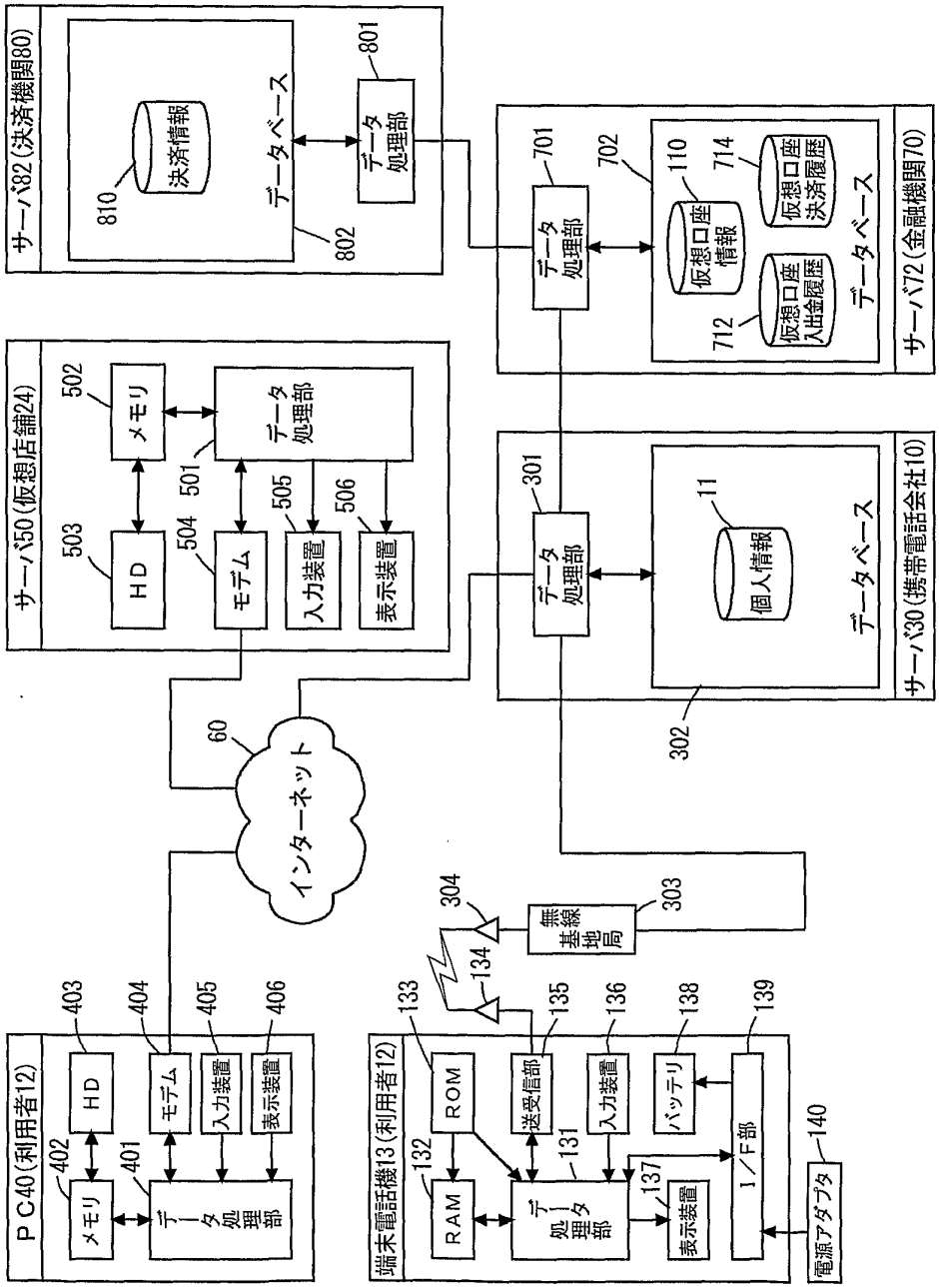

サーバ82(決済機関80)
決済情報
810
データベース
802
データ処理部
801
サーバ50(仮想店舗24)
メモリ
502
HD
503
モデム
504
データ処理部
501
入力装置
505
表示装置
506
サーバ72(金融機関70)
データ処理部
701
702
仮想口座情報
110
仮想口座決済履歴
714
仮想口座入出金履歴
712
データベース
サーバ30(携帯電話会社10)
データ処理部
301
個人情報
11
データベース
302
インターネット
60
PC40(利用者12)
メモリ
402
HD
403
データ処理部
401
モデム
404
入力装置
405
表示装置
406
端末電話機13(利用者12)
RAM
132
ROM
133
データ処理部
131
送受信部
135
入力装置
136
バッテリ
138
表示装置
137
I/F部
139
電源アダプタ
140
無線基地局
303
304
134

FIG. 32

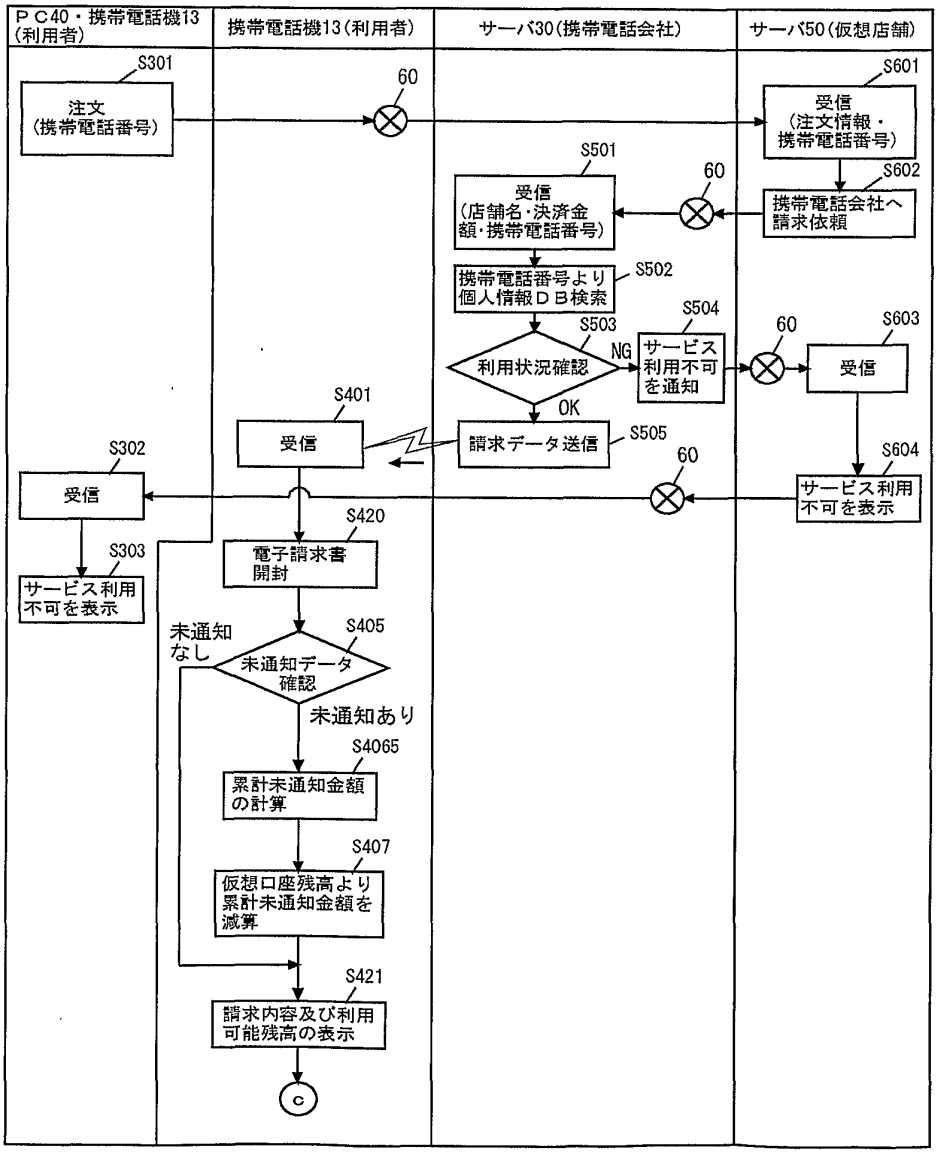

PC40・携帯電話機13(利用者)
携帯電話機13(利用者)
サーバ30(携帯電話会社)
サーバ50(仮想店舗)
S301
注文(携帯電話番号)
60
S601
受信(注文情報・携帯電話番号)
S501
受信(店舗名・決済金額・携帯電話番号)
60
S602
携帯電話会社へ請求依頼
携帯電話番号より個人情報DB検索
S502
S504
S503
利用状況確認
NG
サービス利用不可を通知
60
S603
受信
OK
S401
受信
請求データ送信
S505
60
S604
サービス利用不可を表示
S302
受信
S420
電子請求書開封
S303
サービス利用不可を表示
未通知なし
S405
未通知データ確認
未通知あり
S4065
累計未通知金額の計算
S407
仮想口座残高より累計未通知金額を減算
S421
請求内容及び利用可能残高の表示
C

FIG. 33

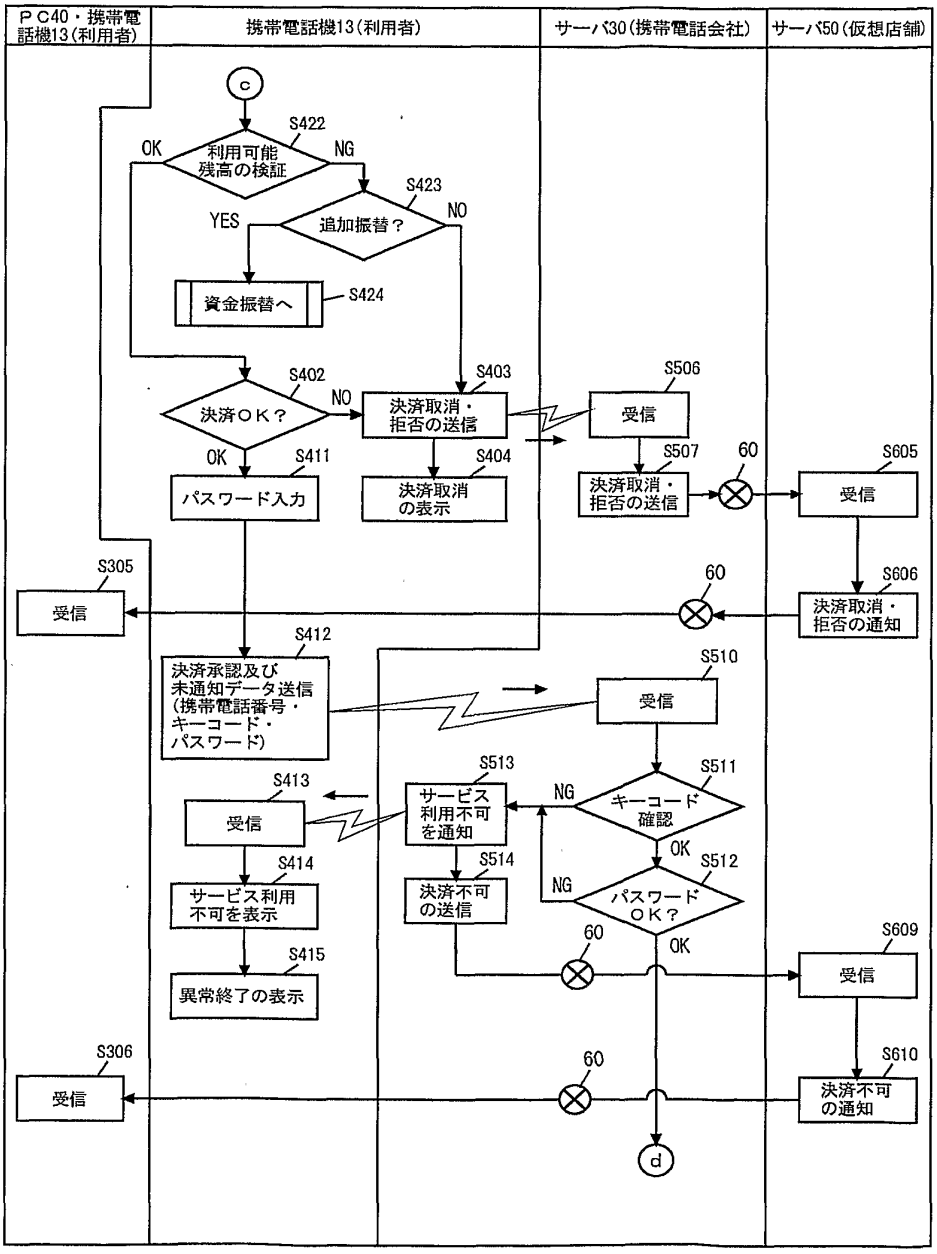
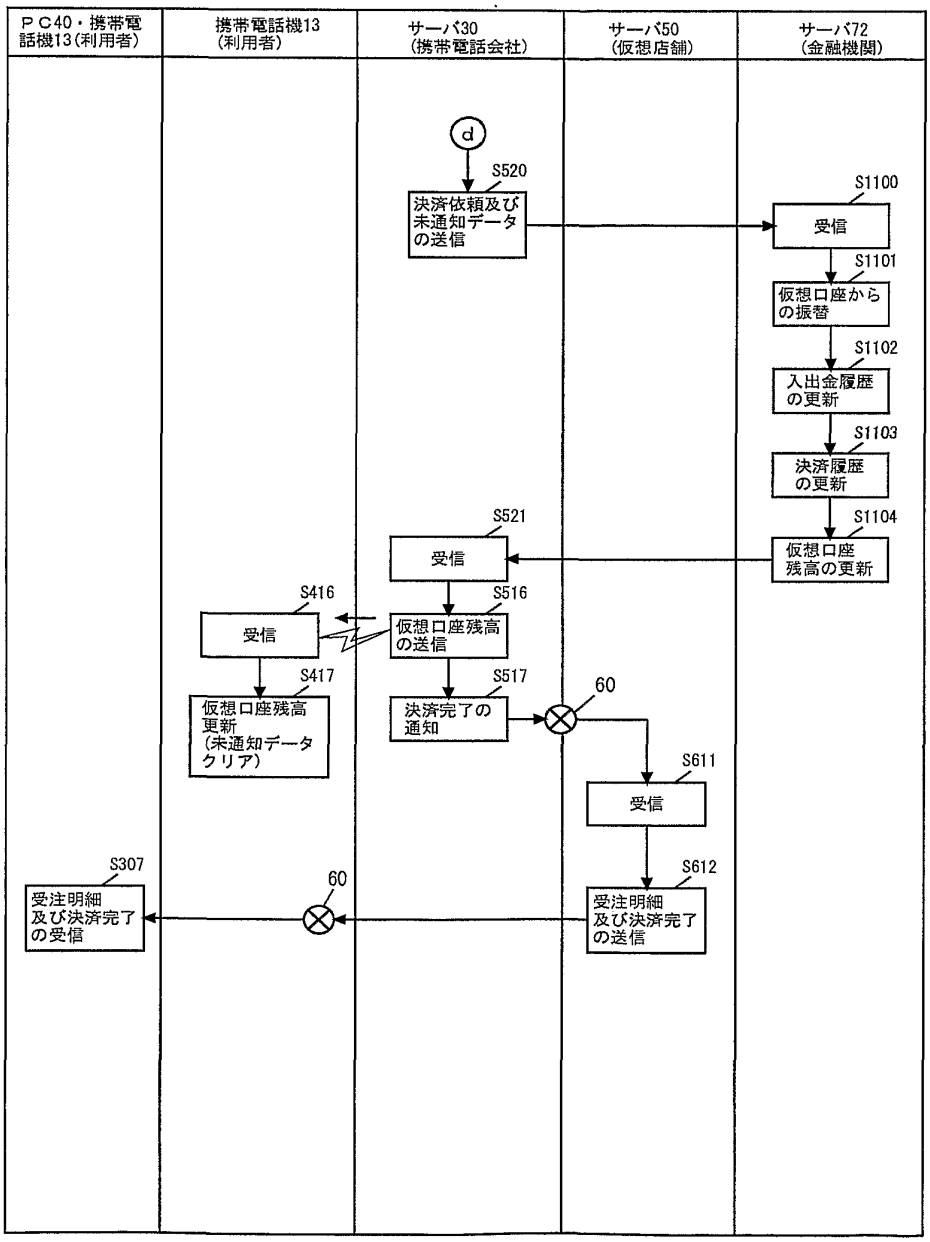

PC40・携帯電話機13(利用者)
携帯電話機13(利用者)
サーバ30(携帯電話会社)
サーバ50(仮想店舗)
c
S422
利用可能残高の検証
OK
NG
S423
追加振替？
YES
NO
資金振替へ
S424
S402
決済OK？
NO
S403
決済取消・拒否の送信
S506
受信
OK
S411
パスワード入力
S404
決済取消の表示
S507
決済取消・拒否の送信
60
S605
受信
S305
受信
60
S606
決済取消・拒否の通知
S412
決済承認及び未通知データ送信(携帯電話番号・キーコード・パスワード)
S510
受信
S513
サービス利用不可を通知
S511
キーコード確認
NG
OK
S413
受信
S512
パスワードOK？
NG
S414
サービス利用不可を表示
S514
決済不可の送信
60
OK
S609
受信
S415
異常終了の表示
S306
受信
60
S610
決済不可の通知
d

FIG. 34



APPL-1002
APPLE INC. / Page 762 of 1892

FIG. 35

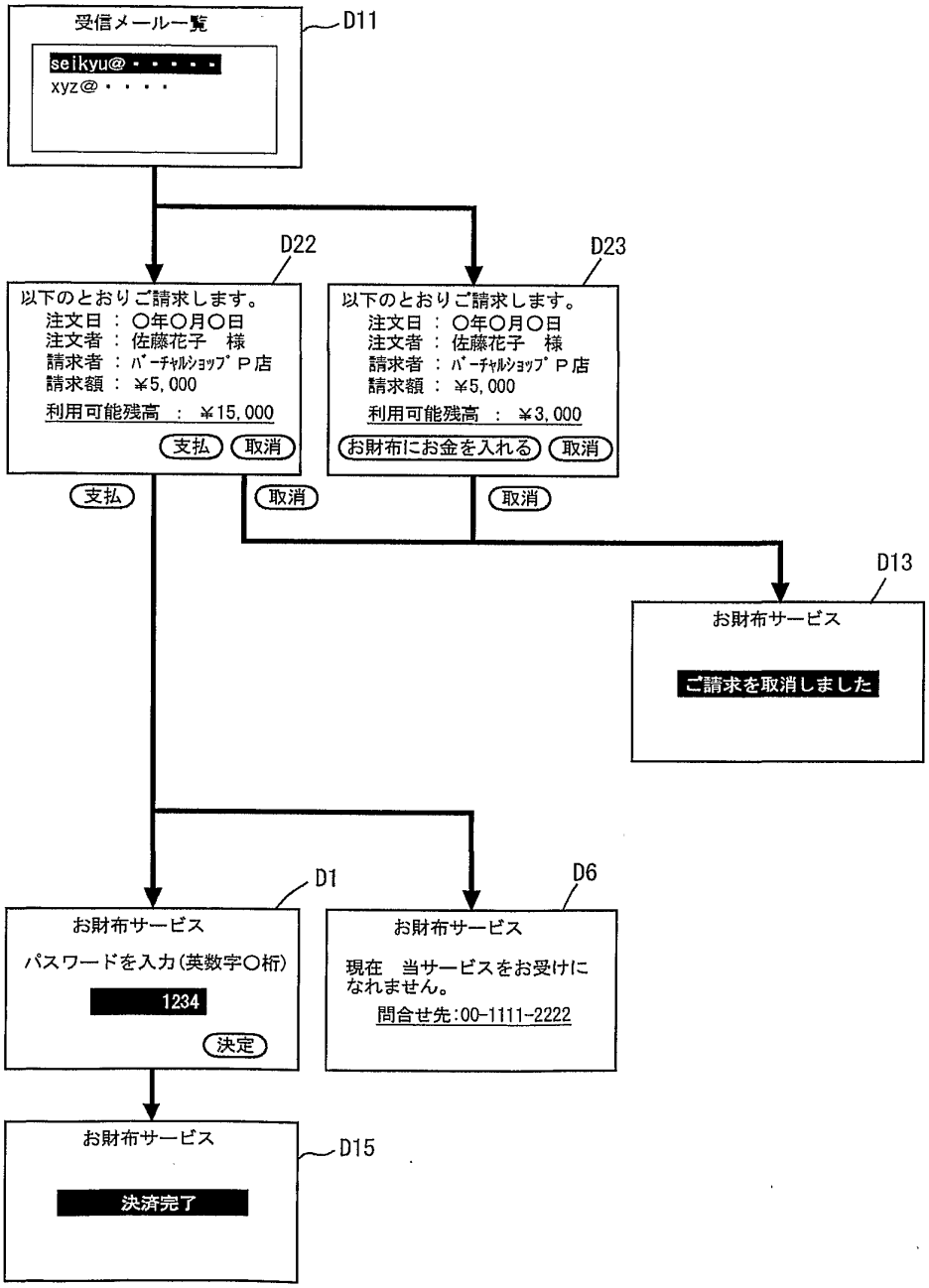

受信メール一覧
D11
seikyu@・・・・・
xyz@・・・・
D22
以下のとおりご請求します。
注文日 : ○年○月○日
注文者 : 佐藤花子 様
請求者 : ﾊﾞｰﾁｬﾙｼｮｯﾌﾟ P店
請求額 : ¥5,000
利用可能残高 : ¥15,000
支払
取消
D23
以下のとおりご請求します。
注文日 : ○年○月○日
注文者 : 佐藤花子 様
請求者 : ﾊﾞｰﾁｬﾙｼｮｯﾌﾟ P店
請求額 : ¥5,000
利用可能残高 : ¥3,000
お財布にお金を入れる
取消
支払
取消
取消
D13
お財布サービス
ご請求を取消しました
D1
お財布サービス
パスワードを入力(英数字○桁)
1234
決定
D6
お財布サービス
現在 当サービスをお受けになれません。
問合せ先:00-1111-2222
お財布サービス
D15
決済完了

FIG. 36

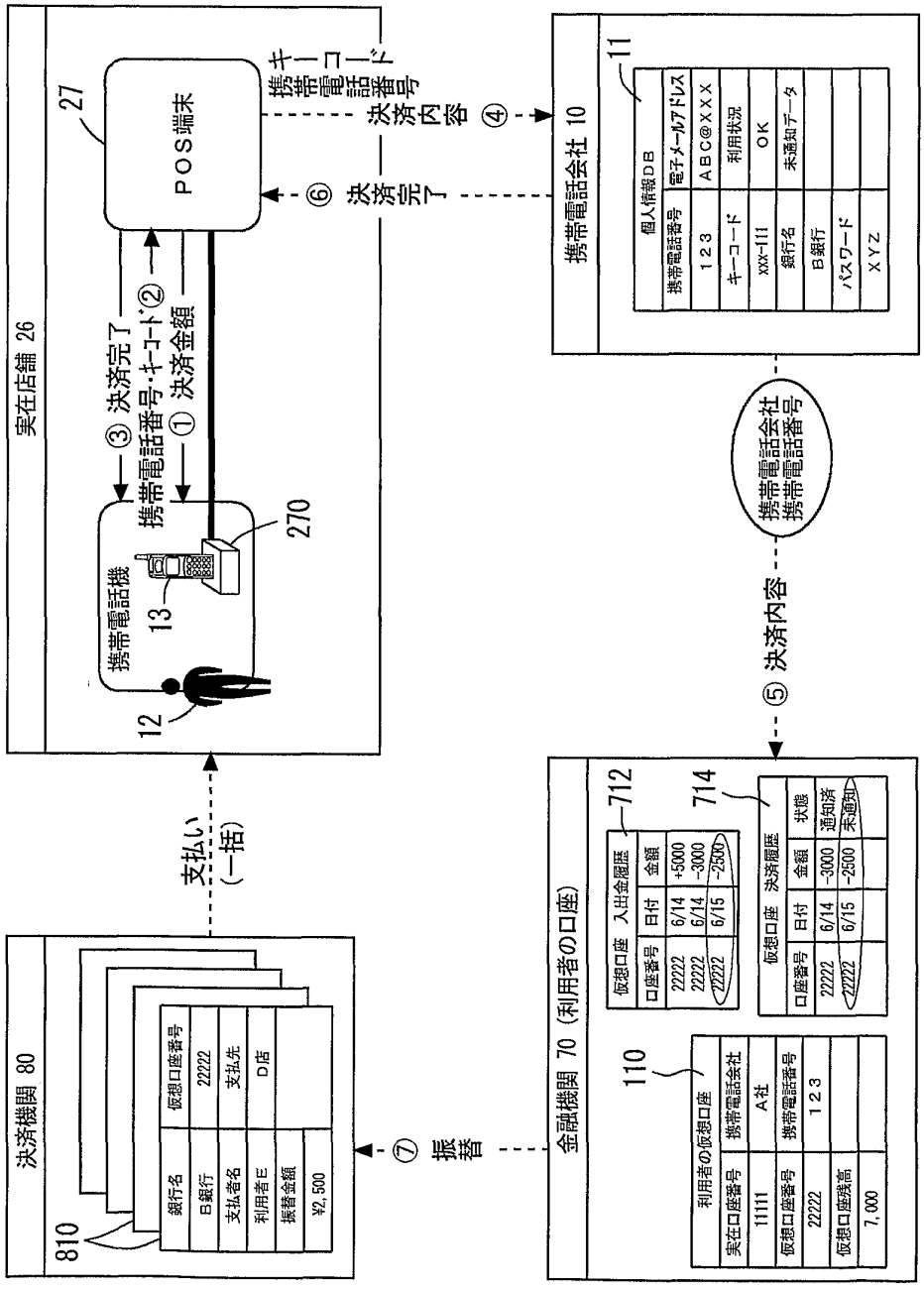

実在店舗 26
27
POS端末
携帯電話機
13
12
270
③ 決済完了
携帯電話番号・キーコード②
① 決済金額
携帯キーコード
携帯電話番号
決済内容 ④
⑥ 決済完了
携帯電話会社 10
11
個人情報DB
携帯電話番号
電子メールアドレス
123
ABC@XXX
キーコード
利用状況
xxx-111
OK
銀行名
未通知データ
B銀行
パスワード
XYZ
携帯電話会社
携帯電話番号
⑤ 決済内容
支払い
(一括)
決済機関 80
810
銀行名
仮想口座番号
B銀行
22222
支払者名
支払先
利用者E
D店
振替金額
¥2,500
⑦ 振替
金融機関 70 (利用者の口座)
110
利用者の仮想口座
実在口座番号
携帯電話会社
11111
A社
仮想口座番号
携帯電話番号
22222
123
仮想口座残高
7,000
712
仮想口座 入出金履歴
口座番号
日付
金額
22222
6/14
+5000
22222
6/14
-3000
22222
6/15
-2500
714
仮想口座 決済履歴
口座番号
日付
金額
状態
22222
6/14
-3000
通知済
22222
6/15
-2500
未通知

FIG. 37

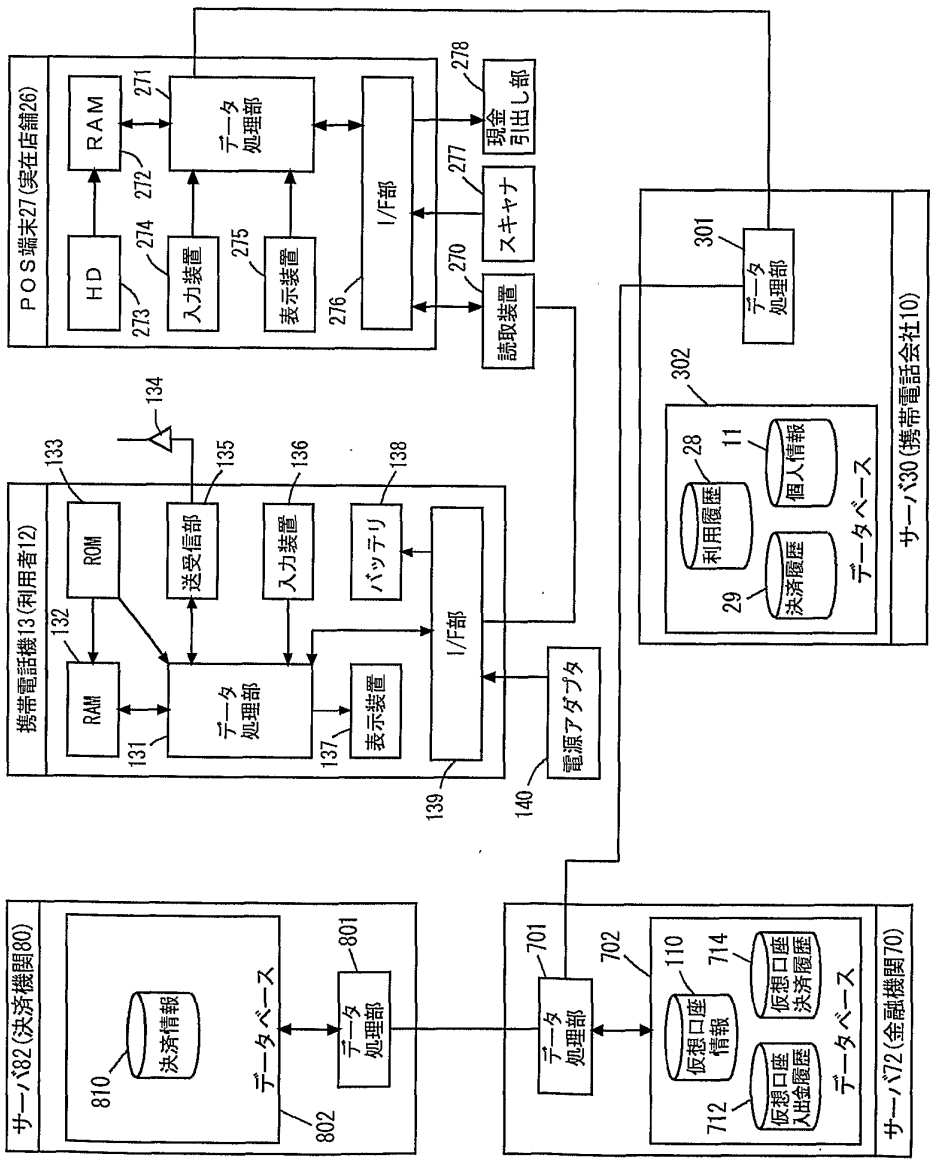

サーバ82(決済機関80)
決済情報
810
データベース
802
データ処理部
801
サーバ72(金融機関70)
データ処理部
701
702
仮想口座情報
110
仮想口座決済履歴
714
仮想口座入出金履歴
712
データベース
携帯電話機13(利用者12)
ROM
133
RAM
132
送受信部
135
入力装置
136
バッテリ
138
データ処理部
131
表示装置
137
I/F部
139
電源アダプタ
140
134
POS端末27(実在店舗26)
HD
273
274
RAM
271
入力装置
275
データ処理部
272
表示装置
276
I/F部
270
278
現金引出し部
277
スキャナ
読取装置
サーバ30(携帯電話会社10)
データ処理部
301
302
利用履歴
28
個人情報
11
決済履歴
29
データベース

FIG. 38

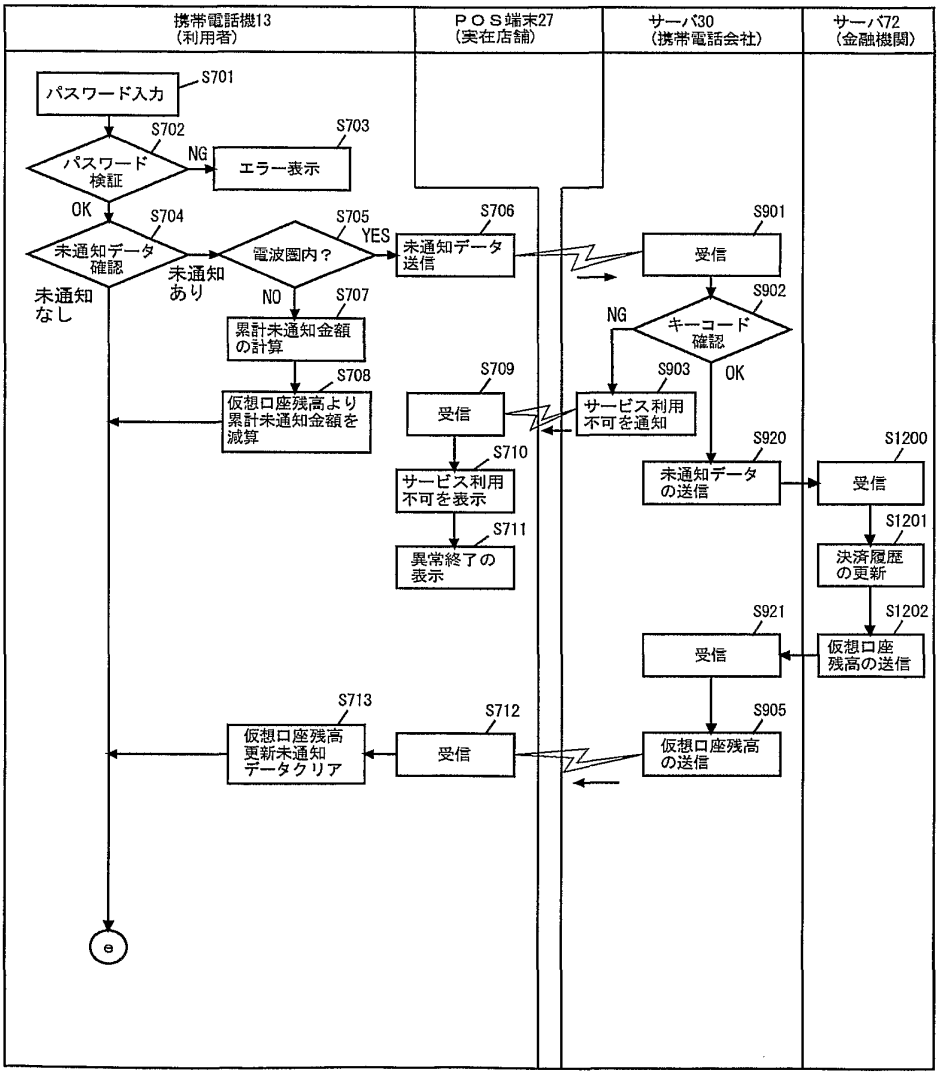

携帯電話機13
(利用者)
POS端末27
(実在店舗)
サーバ30
(携帯電話会社)
サーバ72
(金融機関)
パスワード入力
S701
パスワード検証
S702
NG
S703
エラー表示
OK
未通知データ確認
S704
未通知あり
未通知なし
電波圏内？
S705
YES
NO
S706
未通知データ送信
S707
累計未通知金額の計算
S708
仮想口座残高より累計未通知金額を減算
S709
受信
S710
サービス利用不可を表示
S711
異常終了の表示
S712
受信
S713
仮想口座残高更新未通知データクリア
e
S901
受信
S902
NG
キーコード確認
OK
S903
サービス利用不可を通知
S920
未通知データの送信
S921
受信
S905
仮想口座残高の送信
S1200
受信
S1201
決済履歴の更新
S1202
仮想口座残高の送信

FIG. 39

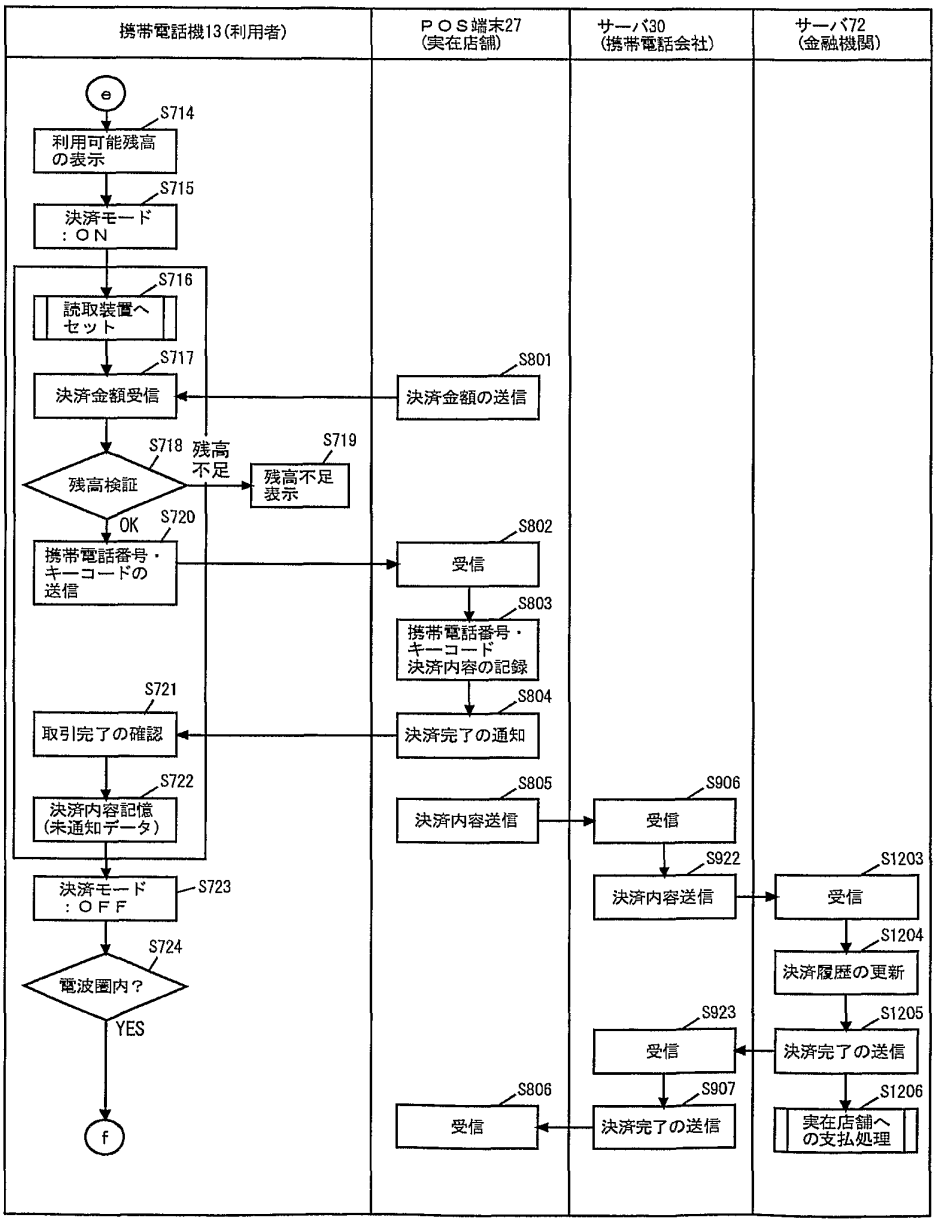

携帯電話機13(利用者)
POS端末27 (実在店舗)
サーバ30 (携帯電話会社)
サーバ72 (金融機関)
e
S714
利用可能残高の表示
S715
決済モード：ON
S716
読取装置へセット
S717
決済金額受信
S801
決済金額の送信
S718
残高検証
残高不足
S719
残高不足表示
OK
S720
携帯電話番号・キーコードの送信
S802
受信
S803
携帯電話番号・キーコード決済内容の記録
S804
決済完了の通知
S721
取引完了の確認
S722
決済内容記憶(未通知データ)
S805
決済内容送信
S906
受信
S922
決済内容送信
S1203
受信
S1204
決済履歴の更新
S1205
決済完了の送信
S923
受信
S907
決済完了の送信
S1206
実在店舗への支払処理
S806
受信
S723
決済モード：OFF
S724
電波圏内？
YES
f

FIG. 40

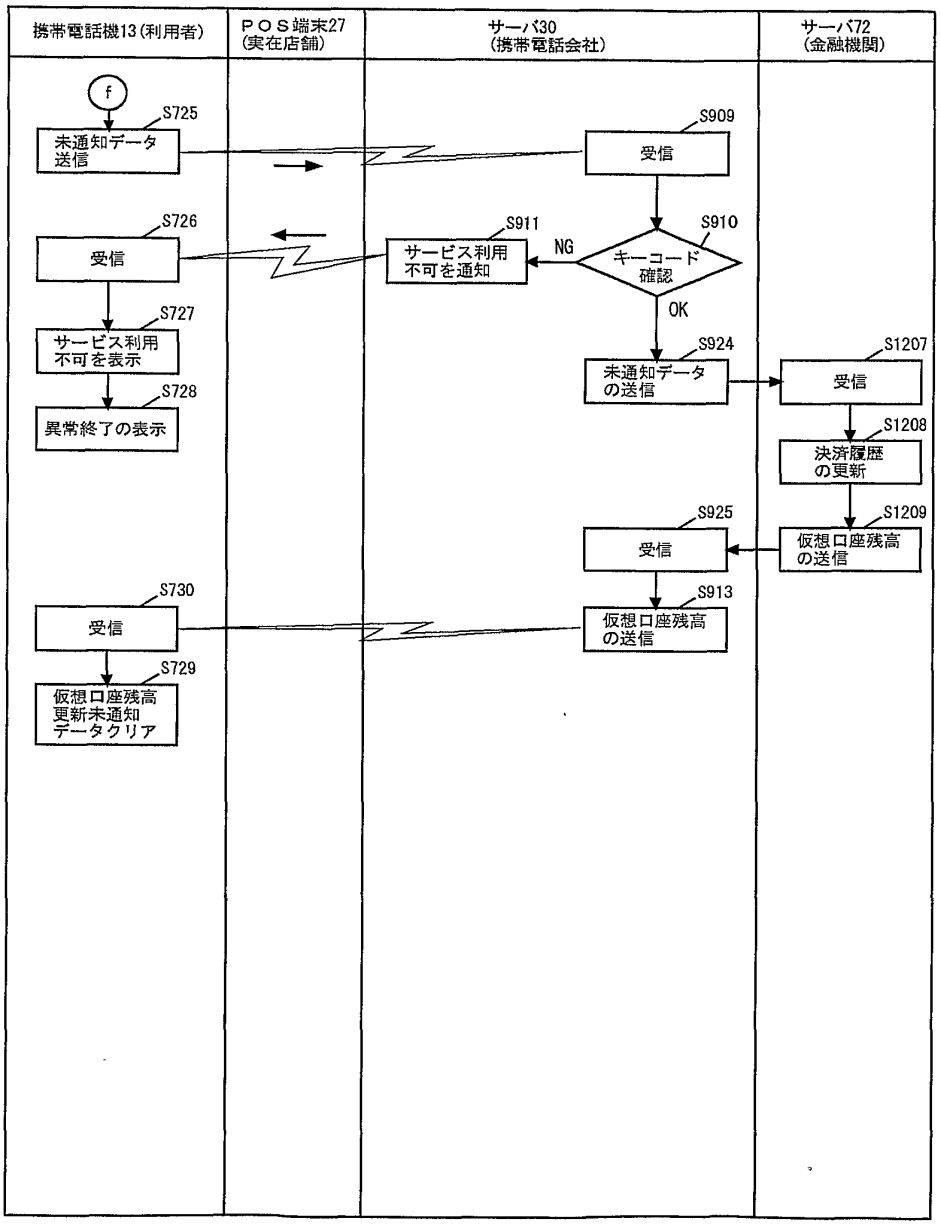

携帯電話機13(利用者)
POS端末27
(実在店舗)
サーバ30
(携帯電話会社)
サーバ72
(金融機関)
f
S725
未通知データ
送信
S726
受信
S727
サービス利用
不可を表示
S728
異常終了の表示
S730
受信
S729
仮想口座残高
更新未通知
データクリア
S909
受信
S911
サービス利用
不可を通知
NG
S910
キーコード
確認
OK
S924
未通知データ
の送信
S925
受信
S913
仮想口座残高
の送信
S1207
受信
S1208
決済履歴
の更新
S1209
仮想口座残高
の送信

FIG. 41

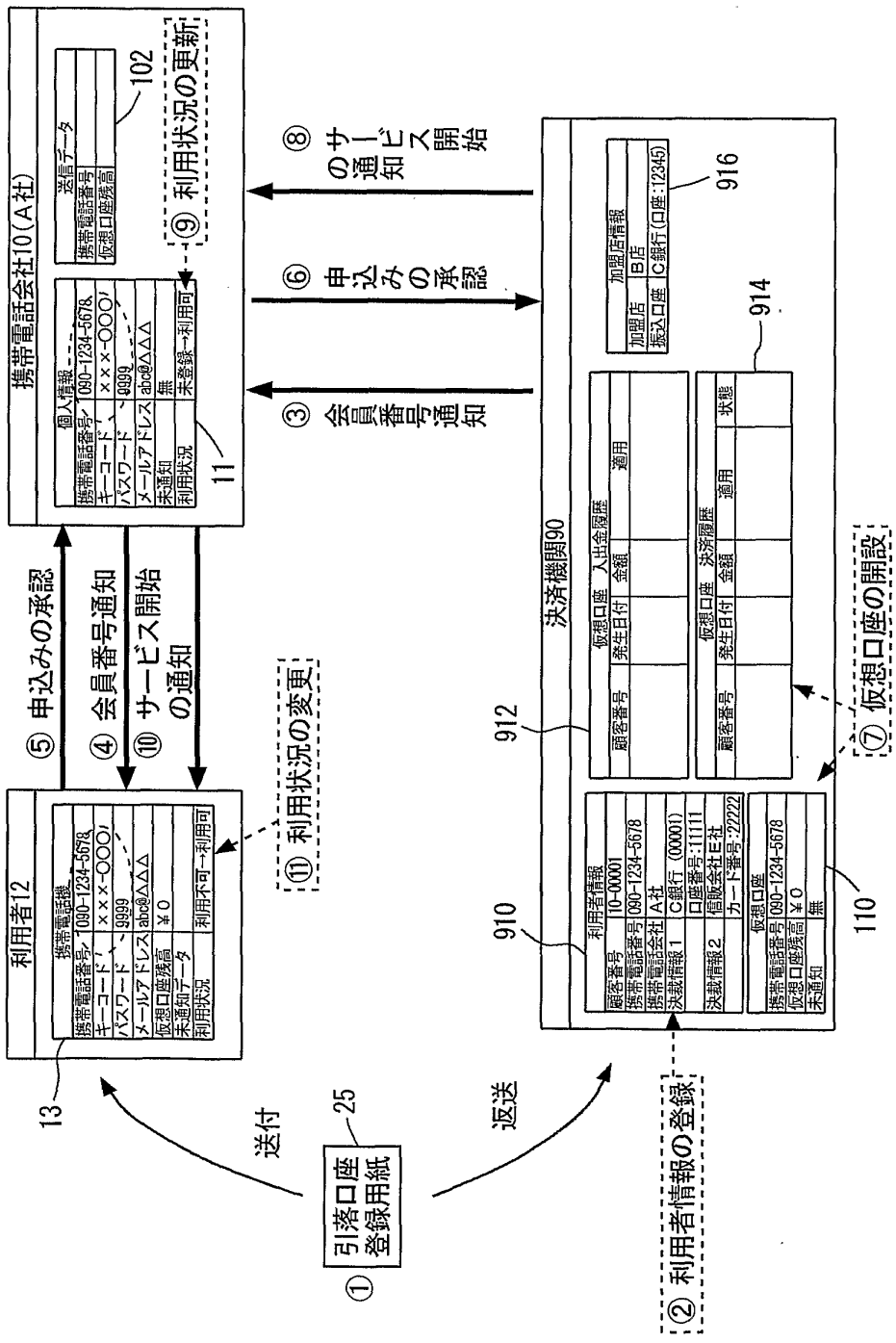

利用者12
携帯電話機
携帯電話番号 090-1234-5678
キーコード ×××-○○○○
パスワード 9999
メールアドレス abc@△△△
仮想口座残高 ¥0
未通知データ
利用状況 利用不可→利用可
13
携帯電話会社10(A社)
個人情報
携帯電話番号 090-1234-5678
キーコード ×××-○○○○
パスワード 9999
メールアドレス abc@△△△
未通知 無
利用状況 未登録→利用可
11
送信データ
携帯電話番号
仮想口座残高
102
⑤ 申込みの承認
④ 会員番号通知
⑩ サービス開始の通知
⑪ 利用状況の変更
⑨ 利用状況の更新
③ 会員番号通知
⑥ 申込みの承認
⑧ サービス開始の通知
決済機関90
912
910
914
916
110
利用者情報
顧客番号 10-00001
携帯電話番号 090-1234-5678
携帯電話会社 A社
決裁情報1 C銀行 (00001)
口座番号:11111
決裁情報2 信販会社E社
カード番号:22222
仮想口座
携帯電話番号 090-1234-5678
仮想口座残高 ¥0
未通知 無
仮想口座 入出金履歴
顧客番号 発生日付 金額 適用
仮想口座 決済履歴
顧客番号 発生日付 金額 適用 状態
加盟店情報
加盟店 B店
振込口座 C銀行(口座:12345)
⑦ 仮想口座の開設
② 利用者情報の登録
① 引落口座登録用紙
25
送付
返送

FIG. 42

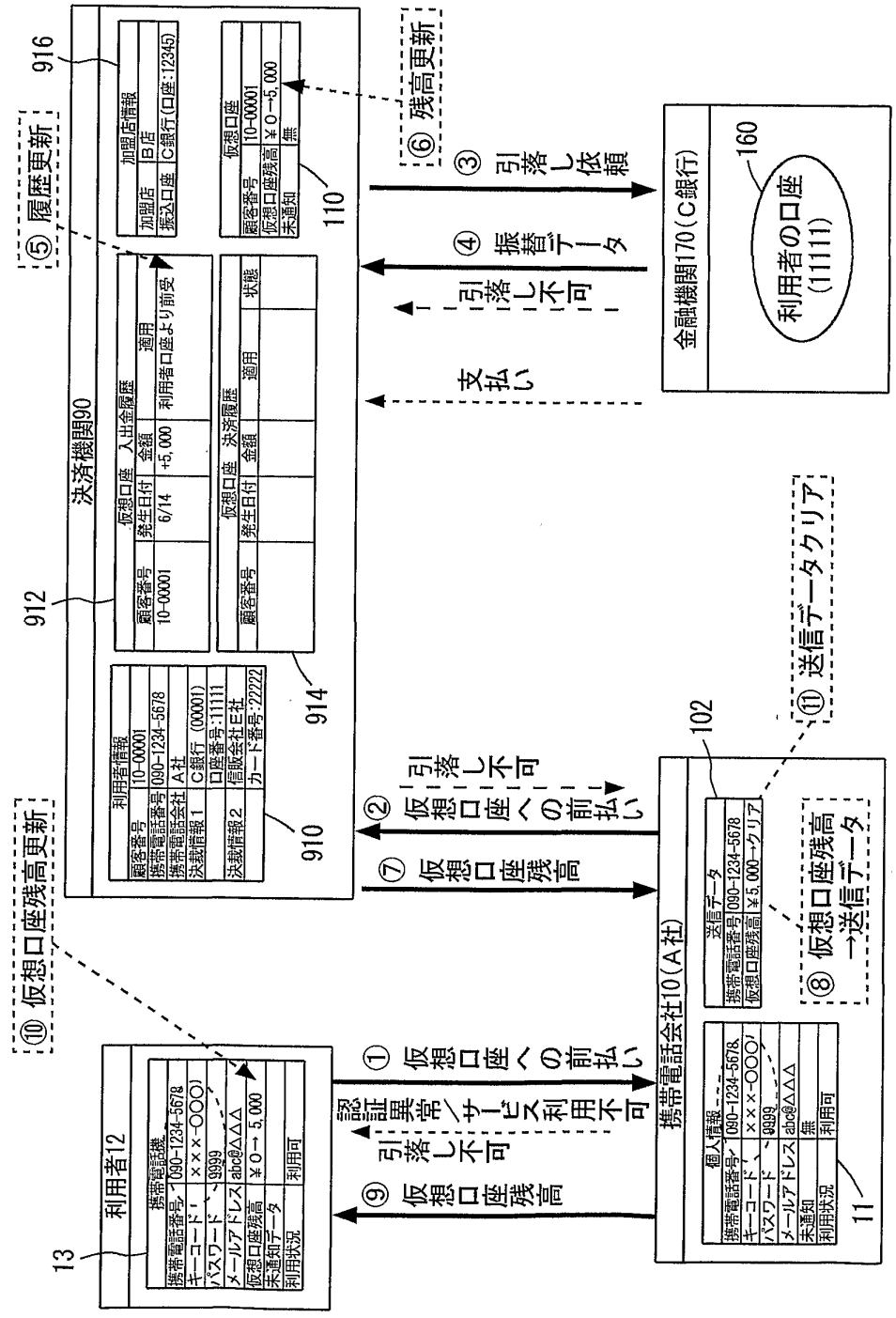

決済機関90
912
914
910
916
110
利用者情報
顧客番号 10-00001
携帯電話番号 090-1234-5678
決裁情報1 A社
C銀行 (00001)
口座番号:11111
決裁情報2 信販会社E社
カード番号:22222
仮想口座 入出金履歴
顧客番号 10-00001
発生日付 6/14
金額 +5,000
適用 利用者口座より前受
仮想口座 決済履歴
顧客番号
発生日付
金額
適用
状態
加盟店情報
加盟店 B店
振込口座 C銀行(口座:12345)
仮想口座
顧客番号 10-00001
仮想口座残高 ¥0→5,000
未通知 無
利用者12
13
携帯電話番号 090-1234-5678
キーコード ××××-○○○○
パスワード 9999
メールアドレス abc@△△△
仮想口座残高 ¥0→5,000
未通知データ
利用状況 利用可
携帯電話会社10(A社)
102
個人情報
携帯電話番号 090-1234-5678
キーコード ××××-○○○○
パスワード 9999
メールアドレス abc@△△△
未通知 無
利用状況 利用可
11
送信データ
携帯電話番号 090-1234-5678
仮想口座残高 ¥5,000→クリア
金融機関170(C銀行)
160
利用者の口座
(11111)
① 仮想口座への前払い
② 仮想口座への前払い
引落し不可
③ 引落し依頼
④ 振替データ
引落し不可
支払い
⑤ 履歴更新
⑥ 残高更新
⑦ 仮想口座残高
⑧ 仮想口座残高→送信データ
⑨ 仮想口座残高
引落し不可
認証異常/サービス利用不可
⑩ 仮想口座残高更新
⑪ 送信データクリア

FIG. 43

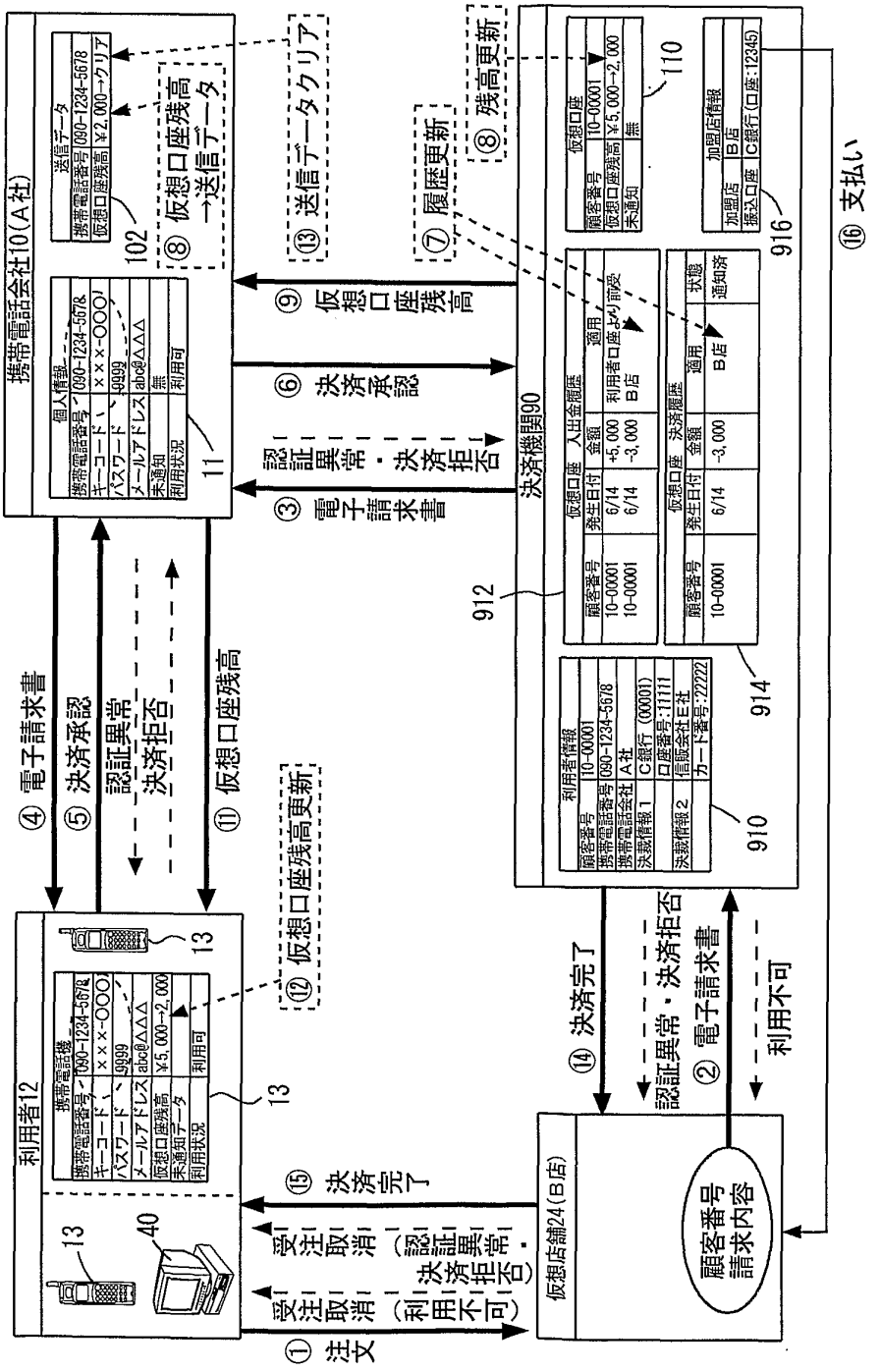
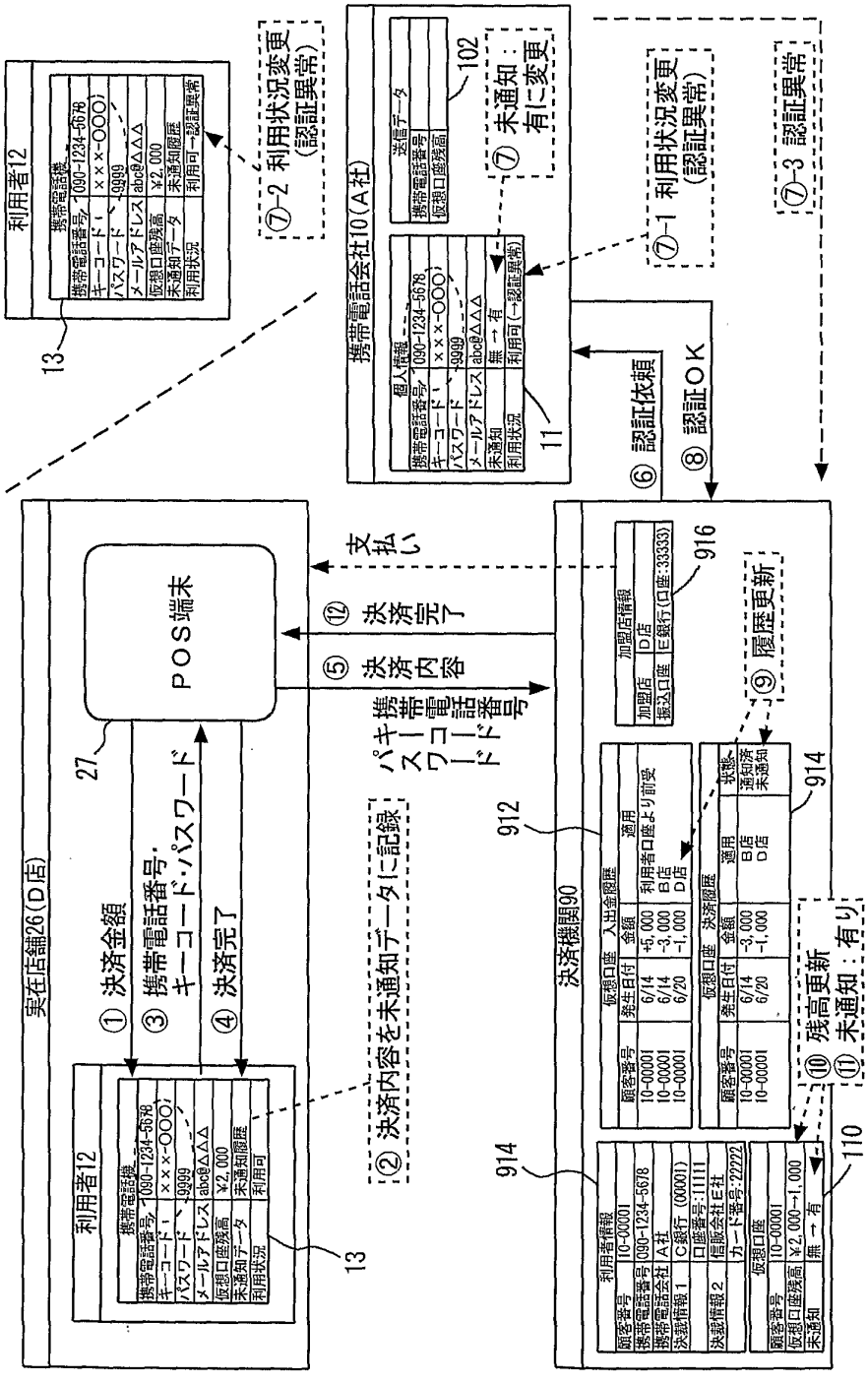

利用者12
携帯電話機
携帯電話番号 090-1234-5678
キーコード ××××-OOO
パスワード 9999
メールアドレス abc@△△△
仮想口座残高 ¥5,000→2,000
未通知データ
利用状況 利用可
13
40
携帯電話会社10(A社)
個人情報
携帯電話番号 090-1234-5678
キーコード ××××-OOO
パスワード 9999
メールアドレス abc@△△△
未通知 無
利用状況 利用可
11
送信データ
携帯電話番号 090-1234-5678
仮想口座残高 ¥2,000→クリア
102
⑧ 仮想口座残高→送信データ
決済機関90
仮想口座 入出金履歴
顧客番号 発生日付 金額 適用
10-00001 6/14 +5,000 利用者口座より前受
10-00001 6/14 -3,000 B店
912
仮想口座 決済履歴
顧客番号 発生日付 金額 適用 状態
10-00001 6/14 -3,000 B店 通知済
914
利用者情報
顧客番号 10-00001
携帯電話番号 090-1234-5678
携帯電話会社 A社
決済情報1 C銀行 (00001)
口座番号:11111
決済情報2 信販会社E社
カード番号:222222
910
仮想口座
顧客番号 10-00001
仮想口座残高 ¥5,000→2,000
未通知 無
110
加盟店情報
加盟店 B店
振込口座 C銀行(口座:12345)
916
仮想店舗24(B店)
顧客番号 請求内容
① 注文
② 電子請求書
③ 電子請求書
④ 電子請求書
⑤ 決済承認
認証異常
決済拒否
⑥ 決済承認
⑦ 履歴更新
⑧ 残高更新
⑨ 仮想口座残高
⑩ 仮想口座残高更新
⑪ 仮想口座残高
⑫ 仮想口座残高更新
⑬ 送信データクリア
⑭ 決済完了
⑮ 決済完了
⑯ 支払い
受注取消(利用不可)
受注取消(認証異常・決済拒否)
認証異常・決済拒否
利用不可

FIG. 44



APPL-1002
APPLE INC. / Page 772 of 1892

FIG. 45

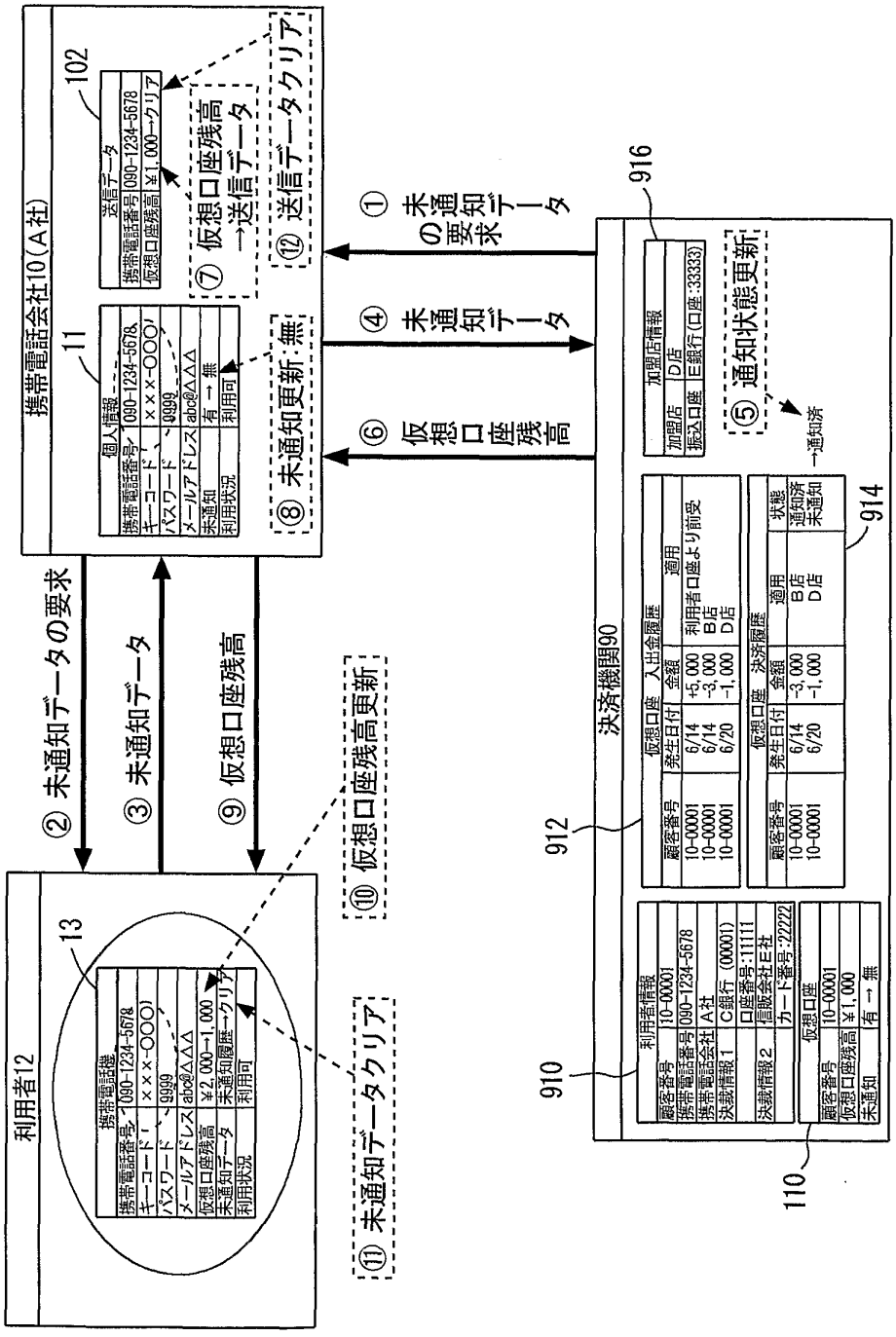
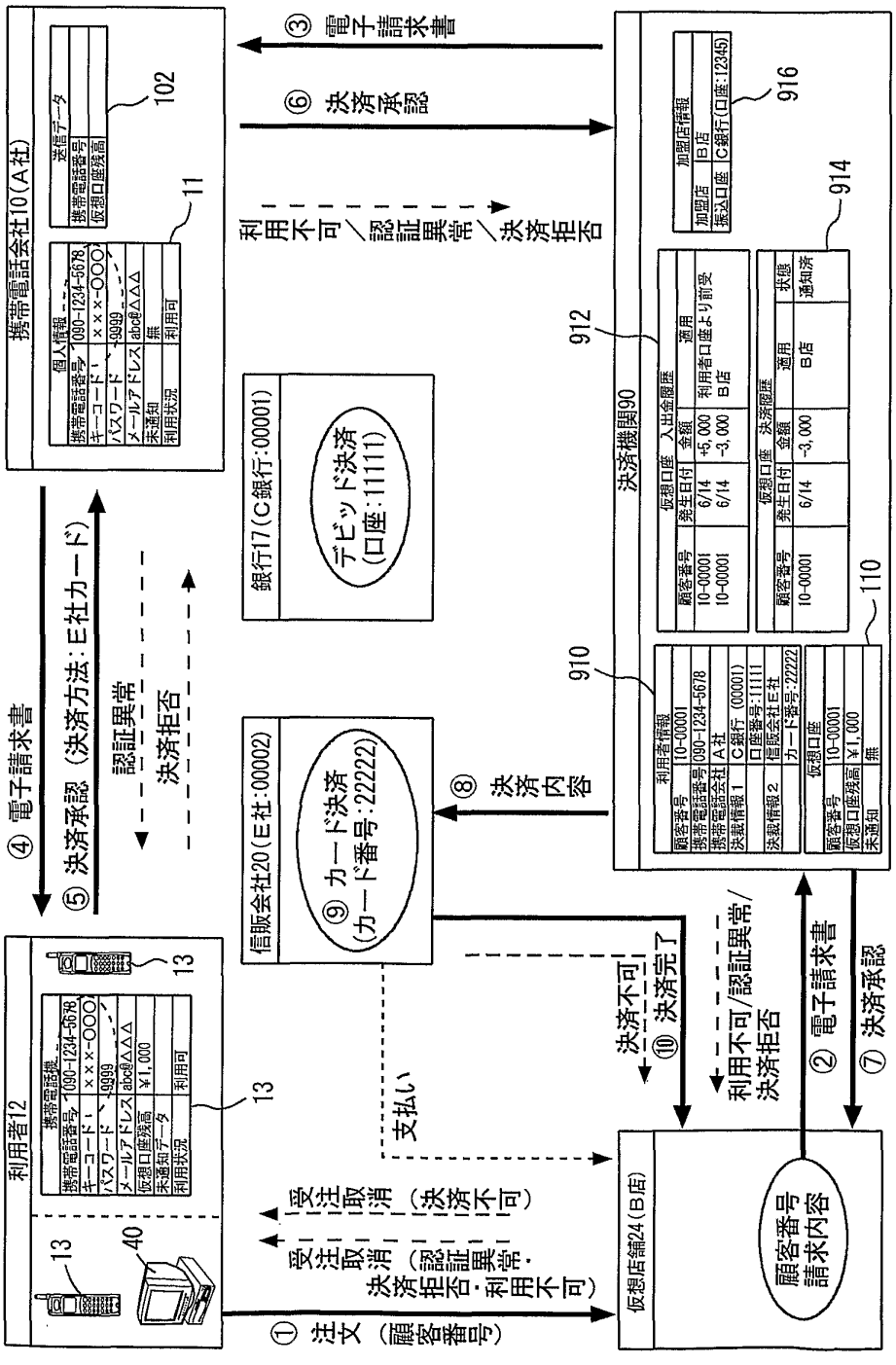

利用者12
13
携帯電話機
携帯電話番号 090-1234-5678
キーコード ×××-OOO
パスワード 9999
メールアドレス abc@△△△
仮想口座残高 ¥2,000→1,000
未通知データ 未通知履歴→クリア
利用状況 利用可
携帯電話会社10(A社)
102
11
個人情報
携帯電話番号 090-1234-5678
キーコード ×××-OOO
パスワード 9999
メールアドレス abc@△△△
未通知 有→無
利用状況 利用可
送信データ
携帯電話番号 090-1234-5678
仮想口座残高 ¥1,000→クリア
② 未通知データの要求
③ 未通知データ
⑨ 仮想口座残高
⑩ 仮想口座残高更新
⑪ 未通知データクリア
⑧ 未通知更新:無
⑦ 仮想口座残高→送信データ
⑫ 送信データクリア
① 未通知データの要求
④ 未通知データ
⑥ 仮想口座残高
⑤ 通知状態更新
→通知済
916
912
910
914
110
決済機関90
利用者情報
顧客番号 10-00001
携帯電話番号 090-1234-5678
携帯電話会社 A社
決裁情報1 C銀行 (00001)
口座番号:11111
決裁情報2 信販会社E社
カード番号:22222
仮想口座
顧客番号 10-00001
仮想口座残高 ¥1,000
未通知 有→無
仮想口座 入出金履歴
顧客番号 発生日付 金額 適用
10-00001 6/14 +5,000 利用者口座より前受
10-00001 6/14 -3,000 B店
10-00001 6/20 -1,000 D店
仮想口座 決済履歴
顧客番号 発生日付 金額 適用 状態
10-00001 6/14 -3,000 B店 通知済
10-00001 6/20 -1,000 D店 未通知
加盟店情報
加盟店 D店
振込口座 E銀行(口座:33333)

FIG. 46



APPL-1002
APPLE INC. / Page 774 of 1892

FIG. 47

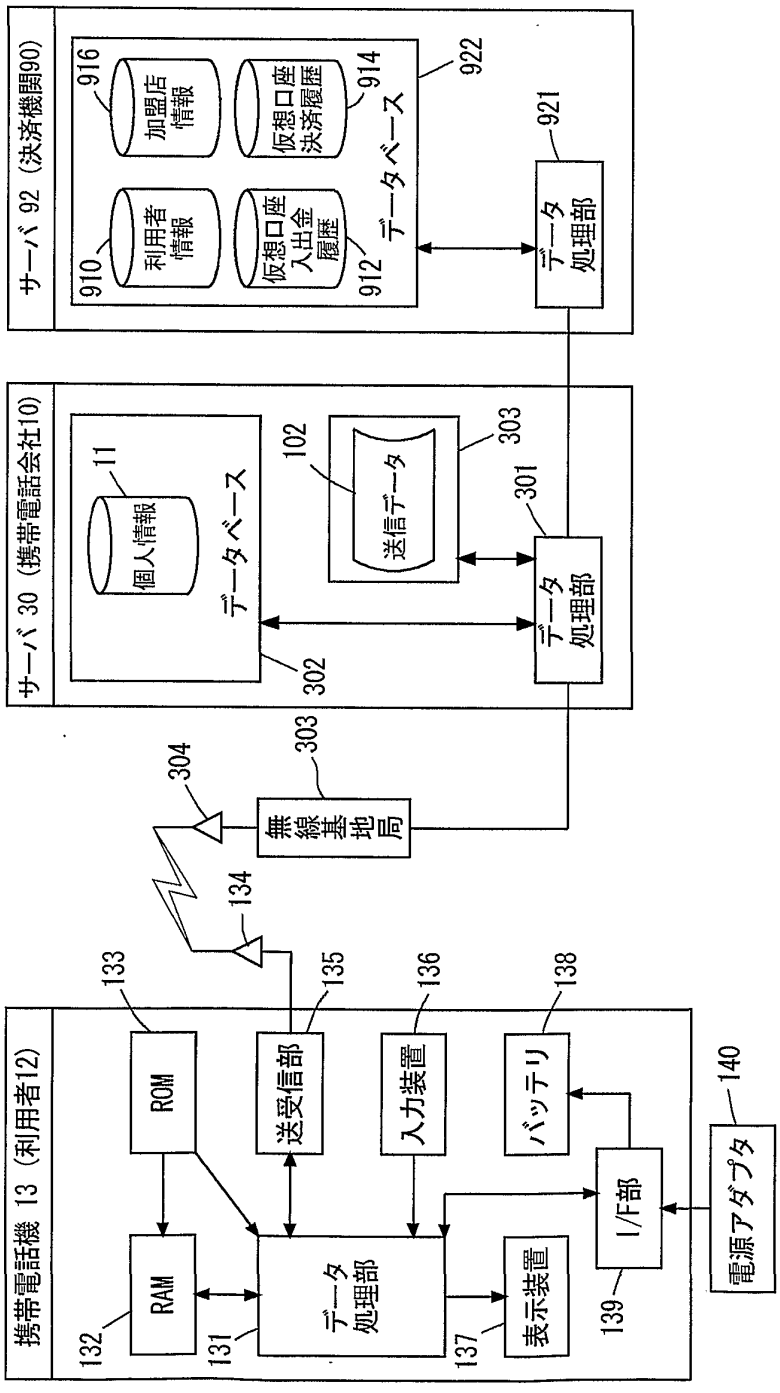

サーバ 92 (決済機関90)
916
加盟店情報
914
仮想口座決済履歴
922
910
利用者情報
912
仮想口座入出金履歴
データベース
921
データ処理部
サーバ 30 (携帯電話会社10)
11
個人情報
データベース
302
102
送信データ
303
301
データ処理部
303
無線基地局
304
134
携帯電話機 13 (利用者12)
133
ROM
135
送受信部
136
入力装置
138
バッテリ
140
電源アダプタ
132
RAM
131
データ処理部
137
表示装置
139
I/F部

FIG. 48

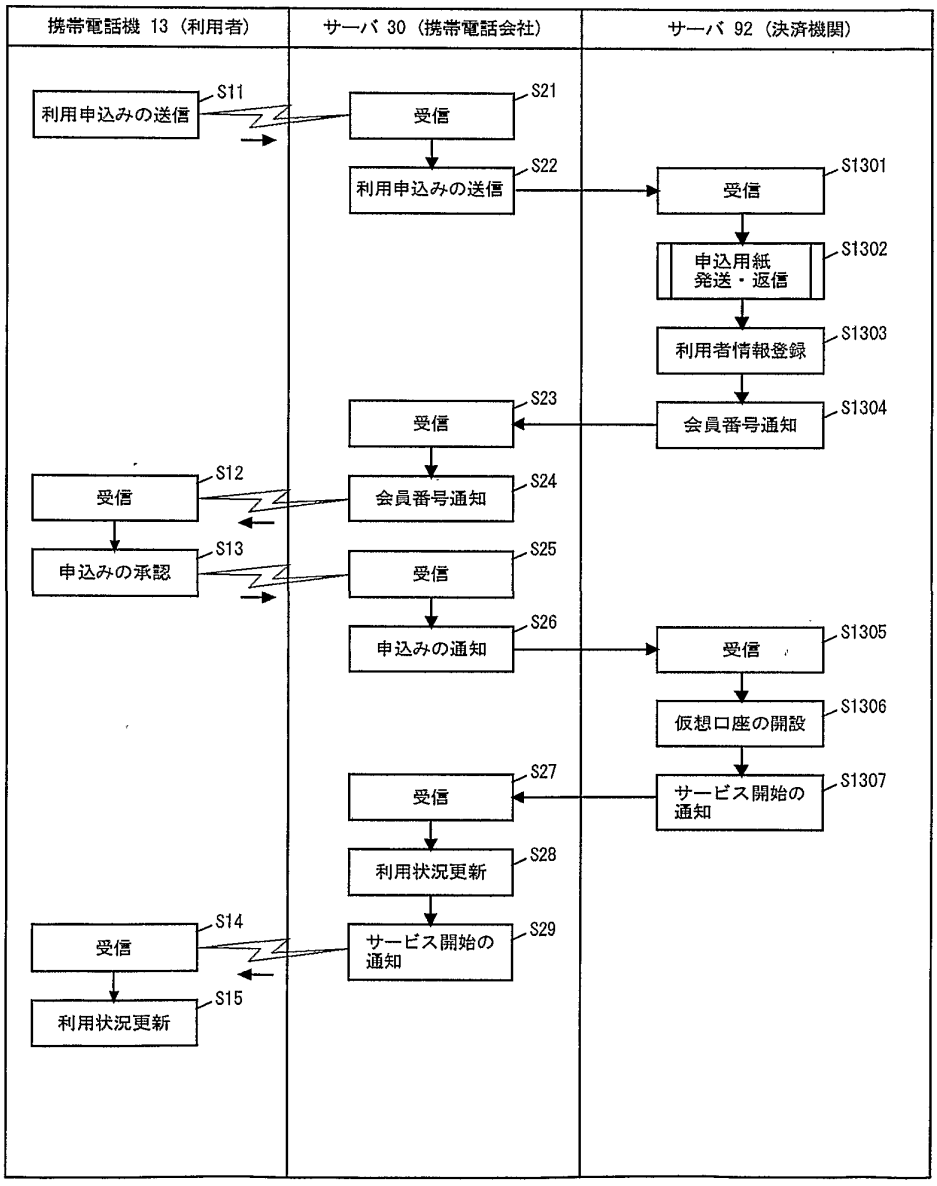

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
利用申込みの送信
S11
受信
S21
利用申込みの送信
S22
受信
S1301
申込用紙
発送・返信
S1302
利用者情報登録
S1303
会員番号通知
S1304
受信
S23
受信
S12
会員番号通知
S24
申込みの承認
S13
受信
S25
申込みの通知
S26
受信
S1305
仮想口座の開設
S1306
受信
S27
サービス開始の
通知
S1307
利用状況更新
S28
受信
S14
サービス開始の
通知
S29
利用状況更新
S15

FIG. 49

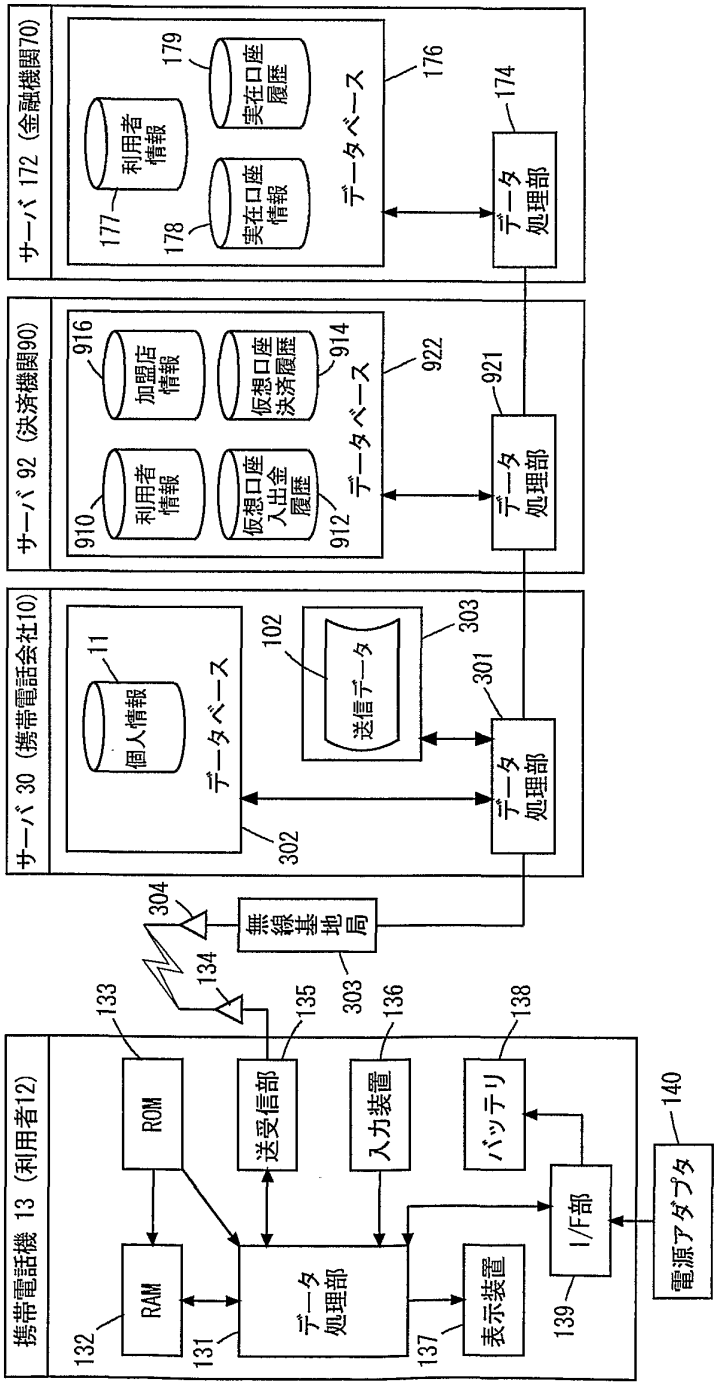

携帯電話機 13 (利用者12)
ROM
RAM
データ処理部
送受信部
入力装置
バッテリ
表示装置
I/F部
電源アダプタ
132
131
133
135
136
137
138
139
140
134
304
無線基地局
303
サーバ 30 (携帯電話会社10)
データベース
個人情報
11
302
送信データ
102
303
データ処理部
301
サーバ 92 (決済機関90)
データベース
利用者情報
910
仮想口座入出金履歴
912
加盟店情報
916
仮想口座決済履歴
914
922
データ処理部
921
サーバ 172 (金融機関70)
データベース
利用者情報
177
実在口座情報
178
実在口座履歴
179
176
データ処理部
174

FIG. 50

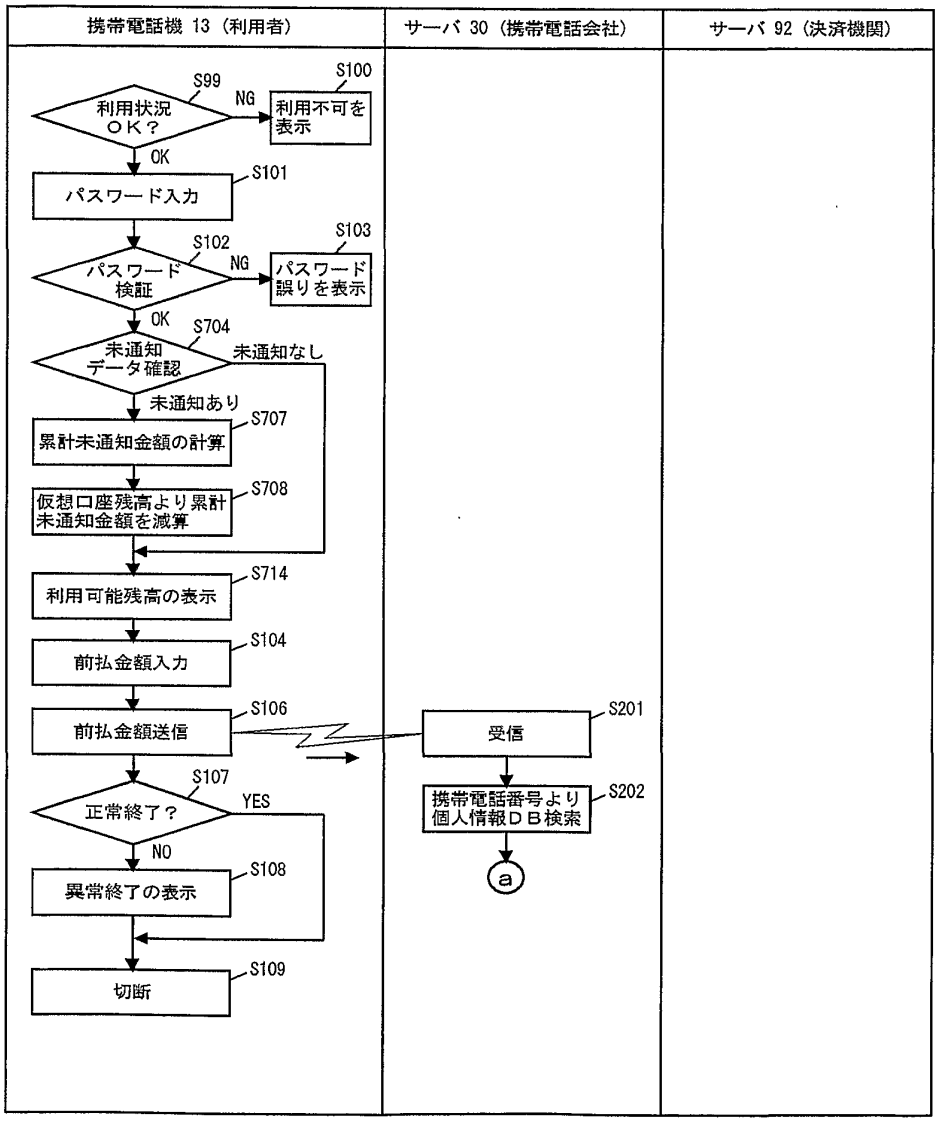

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
S99
利用状況 OK？
NG
S100
利用不可を表示
OK
S101
パスワード入力
S102
パスワード検証
NG
S103
パスワード誤りを表示
OK
S704
未通知データ確認
未通知なし
未通知あり
S707
累計未通知金額の計算
S708
仮想口座残高より累計未通知金額を減算
S714
利用可能残高の表示
S104
前払金額入力
S106
前払金額送信
S201
受信
S202
携帯電話番号より個人情報ＤＢ検索
a
S107
正常終了？
YES
NO
S108
異常終了の表示
S109
切断

FIG. 51

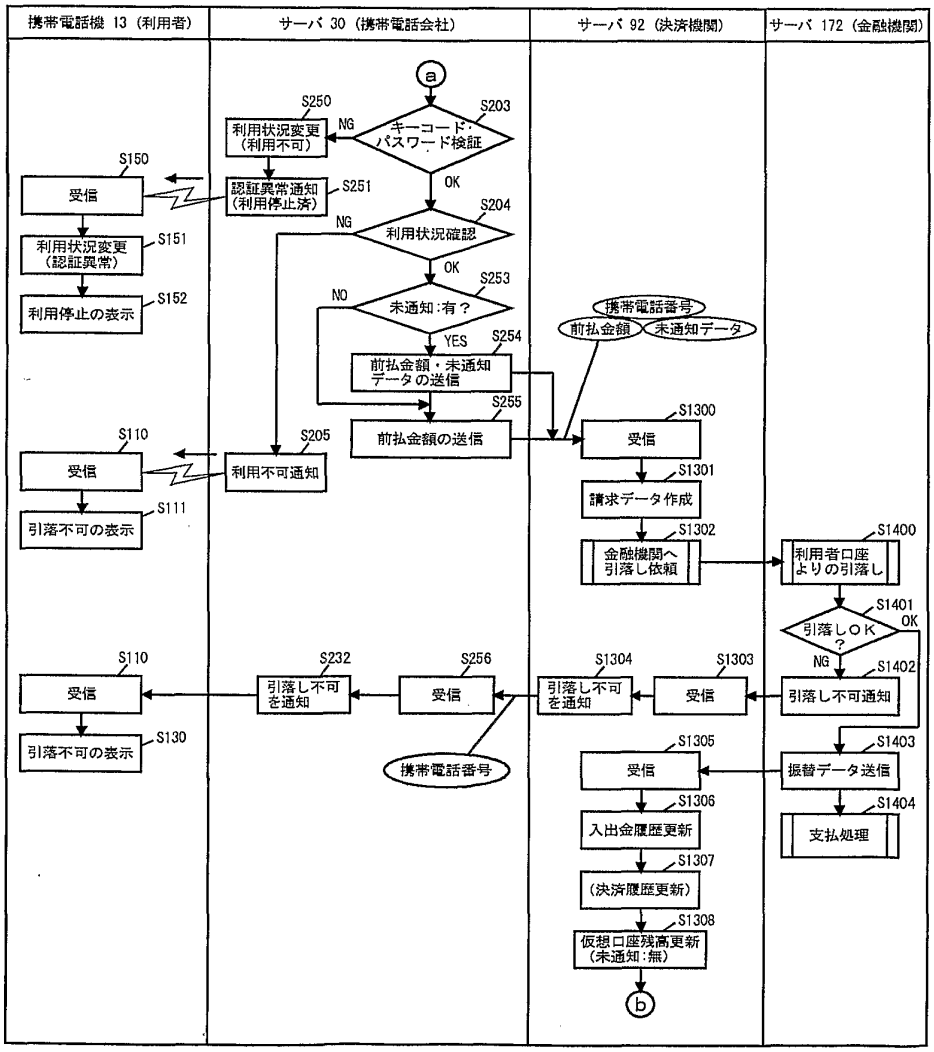

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 172（金融機関）
a
S250
利用状況変更（利用不可）
NG
S203
キーコード・パスワード検証
OK
S150
受信
S251
認証異常通知（利用停止済）
S204
利用状況確認
NG
OK
S151
利用状況変更（認証異常）
S253
未通知：有？
NO
YES
S152
利用停止の表示
携帯電話番号
前払金額
未通知データ
S254
前払金額・未通知データの送信
S255
前払金額の送信
S1300
受信
S110
受信
S205
利用不可通知
S1301
請求データ作成
S111
引落不可の表示
S1302
金融機関へ引落し依頼
S1400
利用者口座よりの引落し
S1401
引落しOK？
OK
NG
S110
受信
S232
引落し不可を通知
S256
受信
S1304
引落し不可を通知
S1303
受信
S1402
引落し不可通知
S130
引落不可の表示
携帯電話番号
S1305
受信
S1403
振替データ送信
S1306
入出金履歴更新
S1404
支払処理
S1307
（決済履歴更新）
S1308
仮想口座残高更新（未通知：無）
b

FIG. 52

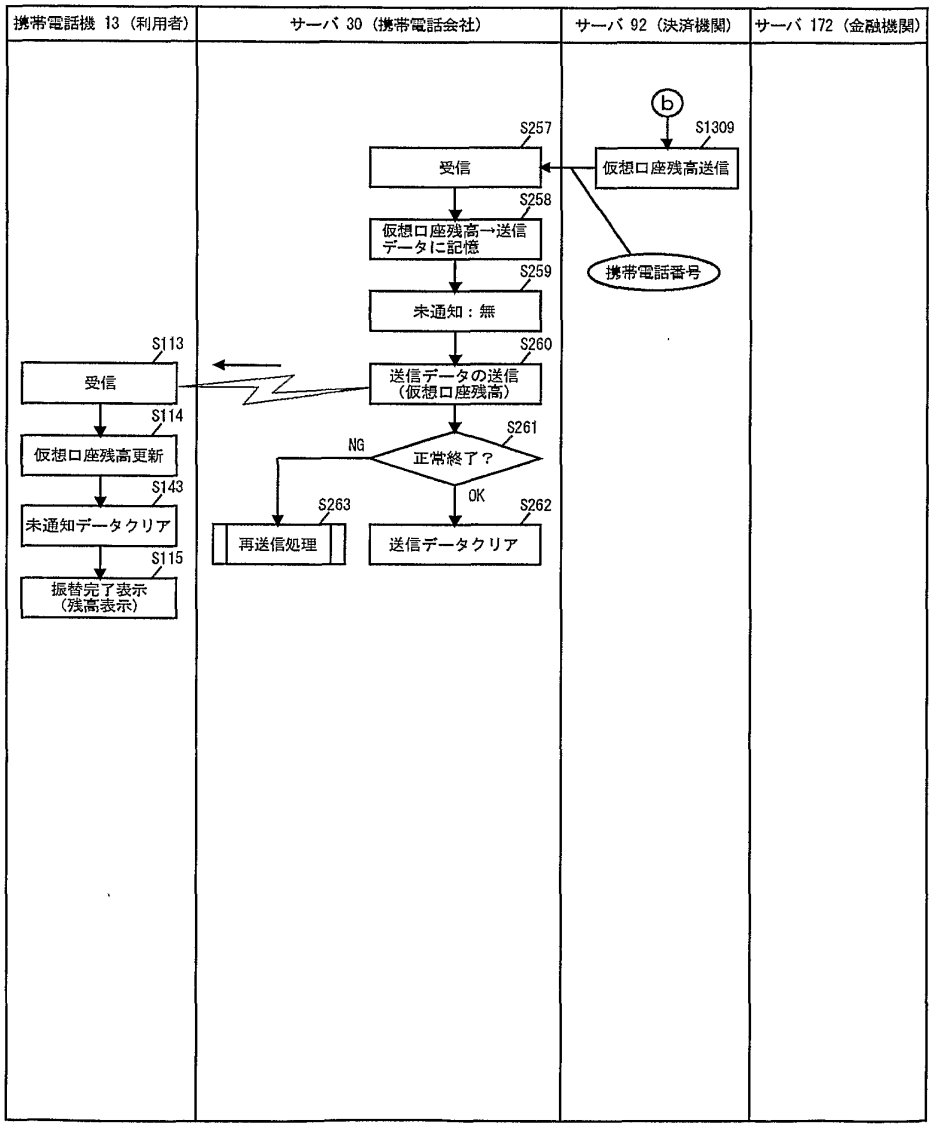
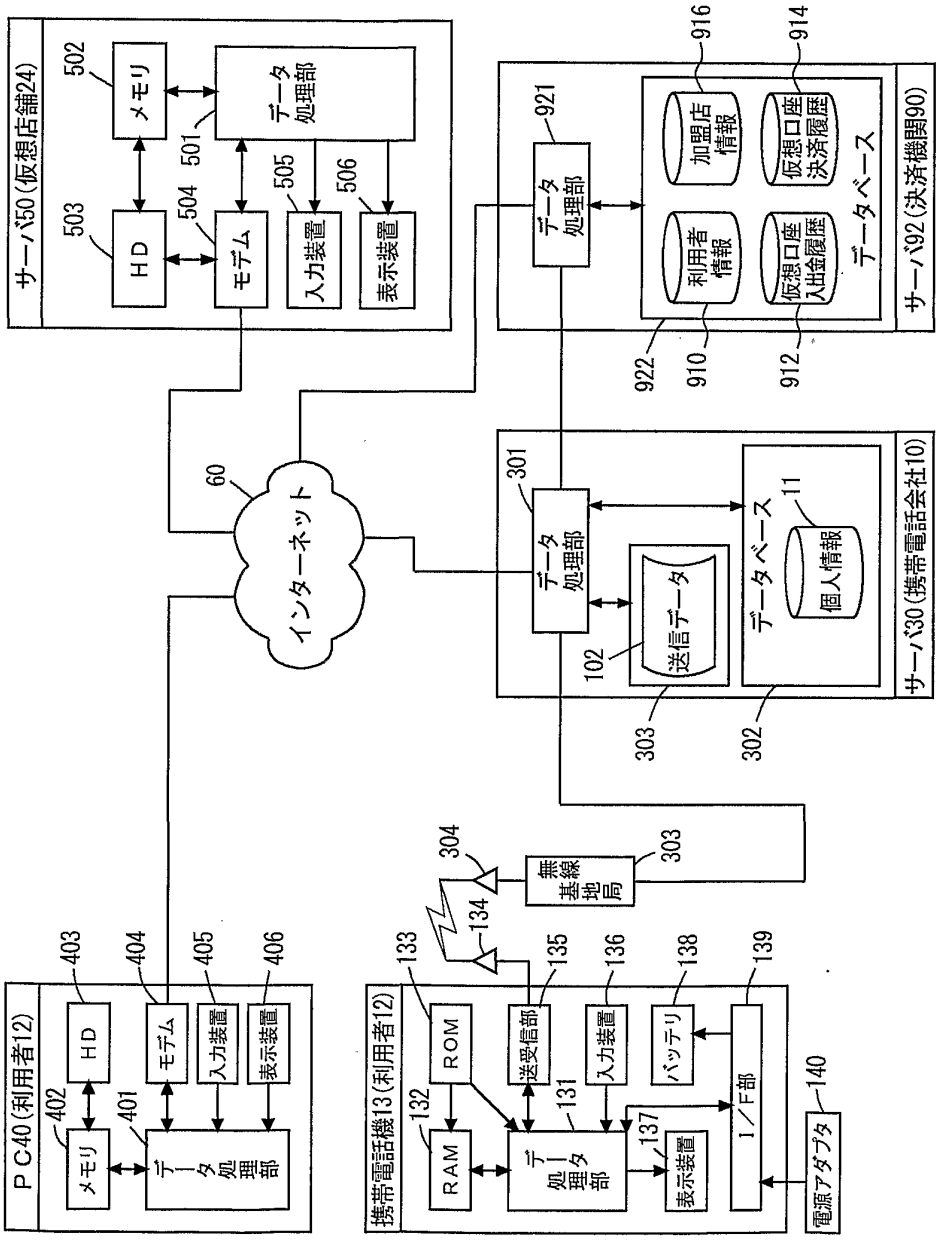

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 172（金融機関）
b
S1309
仮想口座残高送信
携帯電話番号
S257
受信
S258
仮想口座残高→送信データに記憶
S259
未通知：無
S260
送信データの送信（仮想口座残高）
S261
正常終了？
NG
OK
S262
送信データクリア
S263
再送信処理
S113
受信
S114
仮想口座残高更新
S143
未通知データクリア
S115
振替完了表示（残高表示）

FIG. 53



APPL-1002
APPLE INC. / Page 781 of 1892

FIG. 54

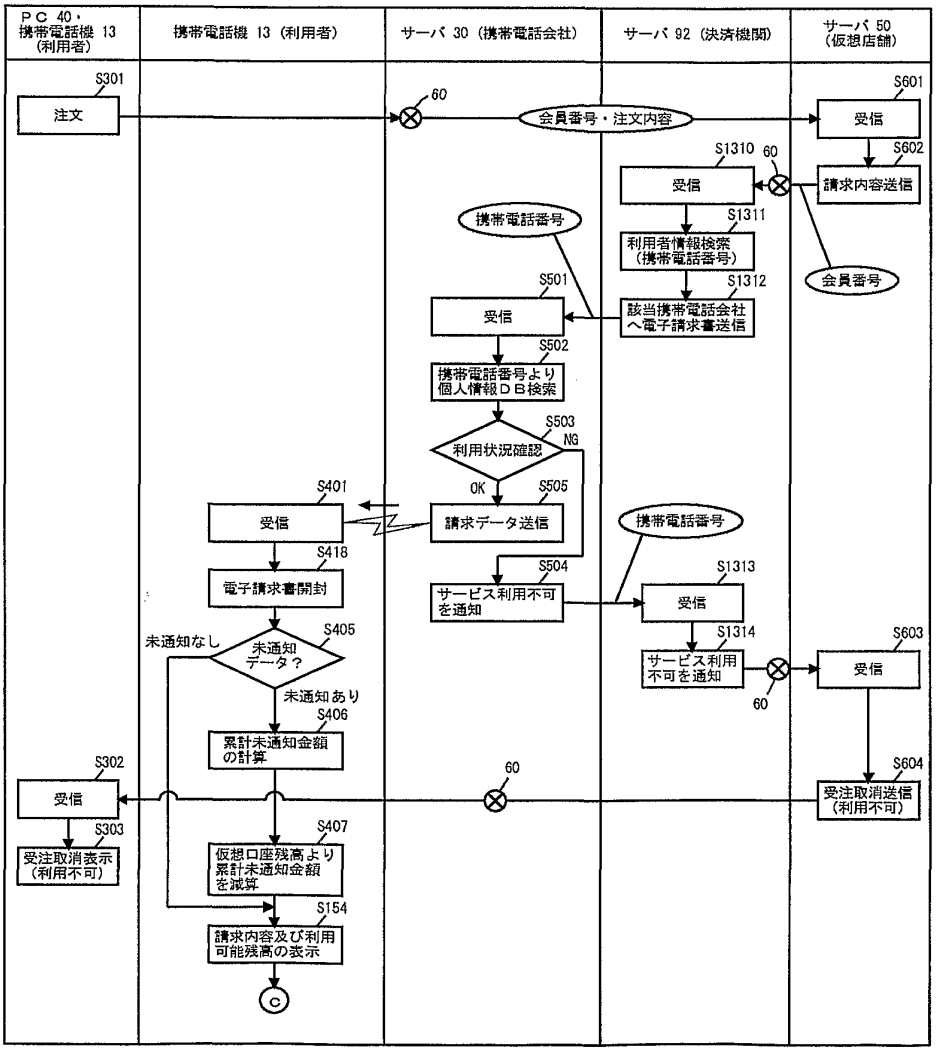

PC 40・携帯電話機 13（利用者）
携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 50（仮想店舗）
S301
注文
60
会員番号・注文内容
S601
受信
S602
請求内容送信
S1310
受信
S1311
利用者情報検索（携帯電話番号）
S1312
該当携帯電話会社へ電子請求書送信
携帯電話番号
会員番号
S501
受信
S502
携帯電話番号より個人情報ＤＢ検索
S503
利用状況確認
NG
OK
S505
請求データ送信
S504
サービス利用不可を通知
S401
受信
S418
電子請求書開封
S405
未通知データ？
未通知なし
未通知あり
S406
累計未通知金額の計算
S407
仮想口座残高より累計未通知金額を減算
S154
請求内容及び利用可能残高の表示
C
携帯電話番号
S1313
受信
S1314
サービス利用不可を通知
60
S603
受信
S604
受注取消送信（利用不可）
60
S302
受信
S303
受注取消表示（利用不可）

FIG. 55

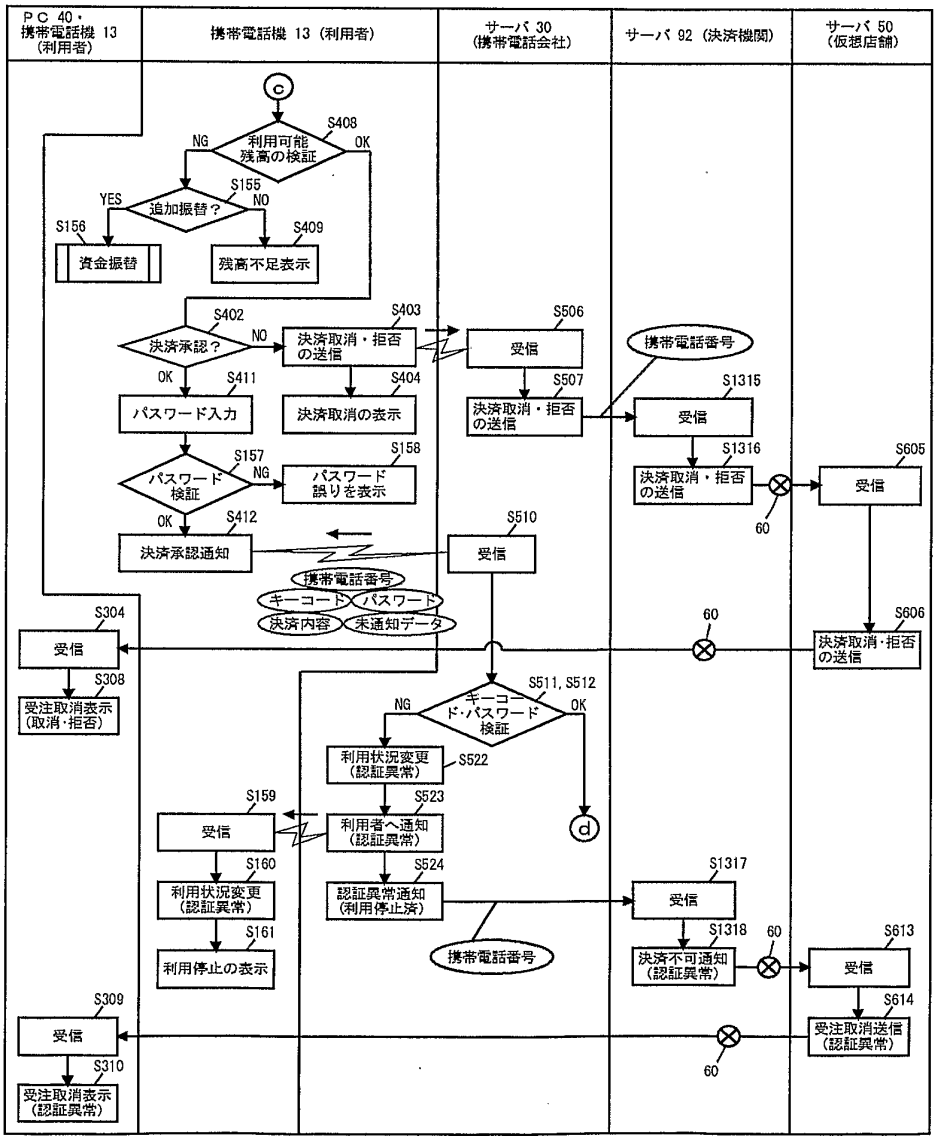

PC 40・携帯電話機 13（利用者）
携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 50（仮想店舗）
c
S408
利用可能残高の検証
NG
OK
S155
追加振替？
YES
NO
S156
資金振替
S409
残高不足表示
S402
決済承認？
NO
S403
決済取消・拒否の送信
S506
受信
携帯電話番号
OK
S411
パスワード入力
S404
決済取消の表示
S507
決済取消・拒否の送信
S1315
受信
S157
パスワード検証
NG
S158
パスワード誤りを表示
S1316
決済取消・拒否の送信
60
S605
受信
OK
S412
決済承認通知
S510
受信
携帯電話番号
キーコード
パスワード
決済内容
未通知データ
60
S606
決済取消・拒否の送信
S304
受信
S308
受注取消表示（取消・拒否）
S511, S512
キーコード・パスワード検証
NG
OK
利用状況変更（認証異常）
S522
S159
受信
S523
利用者へ通知（認証異常）
d
S160
利用状況変更（認証異常）
S524
認証異常通知（利用停止済）
S1317
受信
S161
利用停止の表示
携帯電話番号
S1318
決済不可通知（認証異常）
60
S613
受信
S309
受信
S614
受注取消送信（認証異常）
60
S310
受注取消表示（認証異常）

FIG. 56

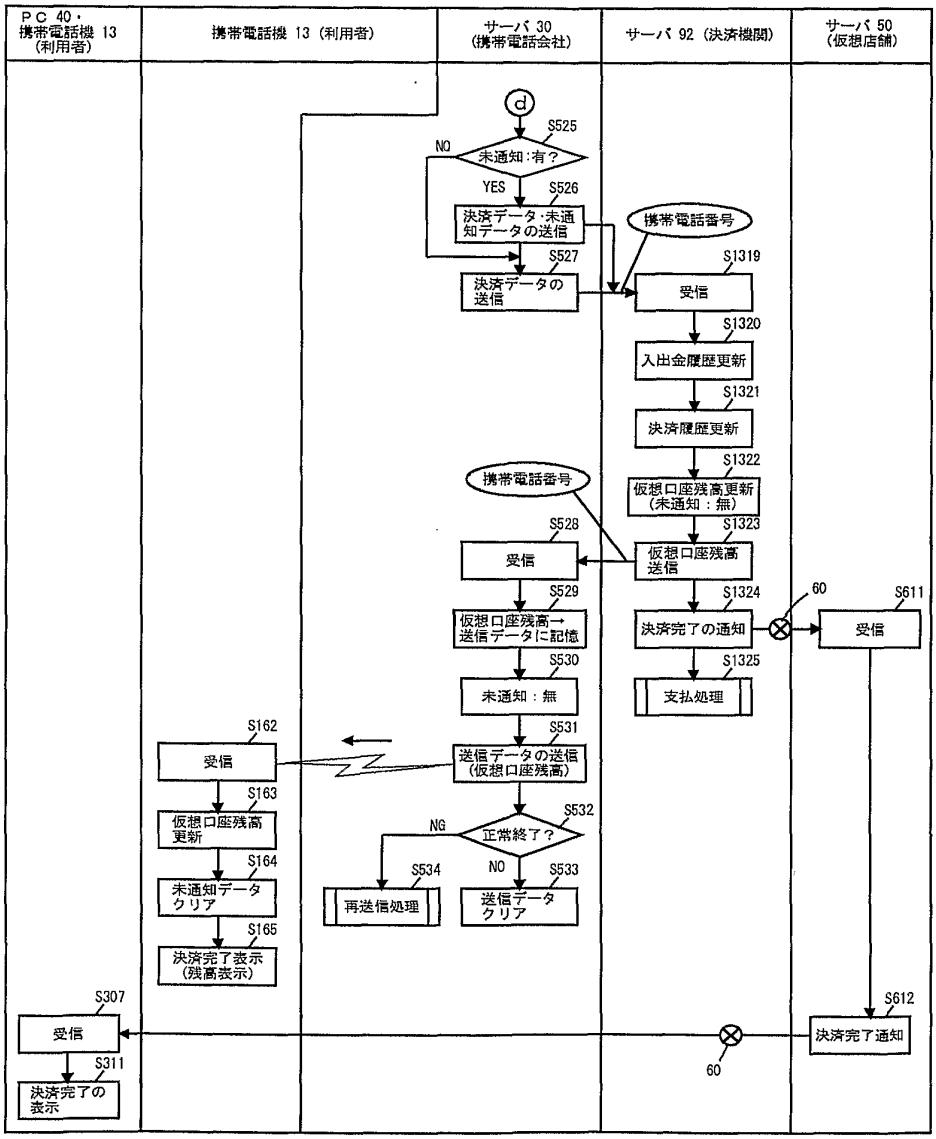

PC 40・携帯電話機 13（利用者）
携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 50（仮想店舗）
d
S525
未通知：有？
NO
YES
S526
決済データ・未通知データの送信
携帯電話番号
S527
決済データの送信
S1319
受信
S1320
入出金履歴更新
S1321
決済履歴更新
S1322
仮想口座残高更新（未通知：無）
携帯電話番号
S528
受信
S1323
仮想口座残高送信
S529
仮想口座残高→送信データに記憶
S1324
決済完了の通知
60
S611
受信
S530
未通知：無
S1325
支払処理
S162
受信
S531
送信データの送信（仮想口座残高）
S163
仮想口座残高更新
S532
正常終了？
NG
NO
S534
再送信処理
S533
送信データクリア
S164
未通知データクリア
S165
決済完了表示（残高表示）
S307
受信
S311
決済完了の表示
60
S612
決済完了通知

FIG. 57

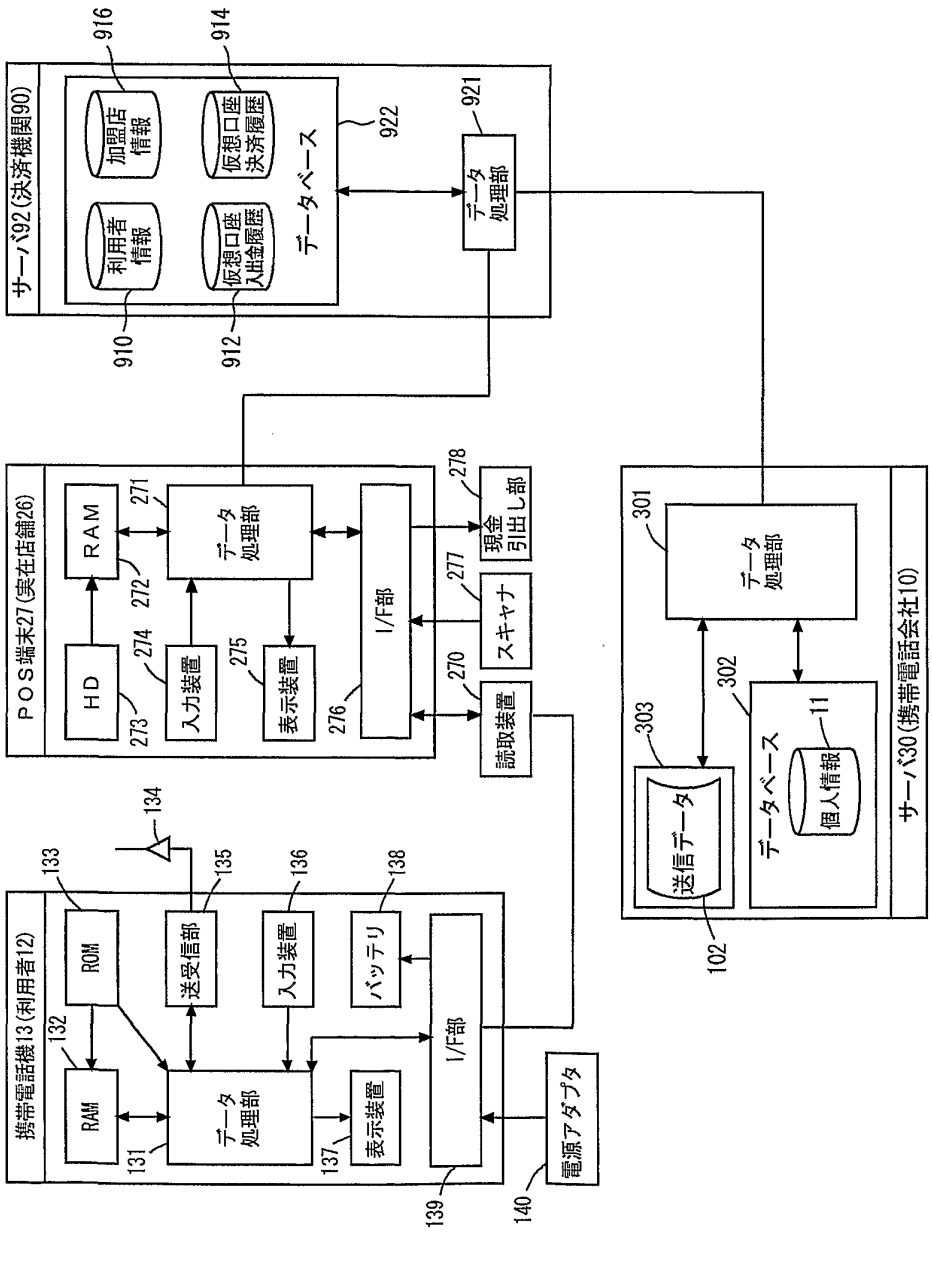

サーバ92(決済機関90)
916
914
加盟店情報
仮想口座決済履歴
利用者情報
仮想口座入出金履歴
データベース
922
921
データ処理部
910
912
POS端末27(実在店舗26)
RAM
271
HD
272
データ処理部
274
入力装置
273
275
表示装置
276
I/F部
278
現金引出し部
277
スキャナ
270
読取装置
携帯電話機13(利用者12)
134
133
ROM
135
送受信部
136
入力装置
138
バッテリ
132
RAM
データ処理部
131
137
表示装置
I/F部
139
140
電源アダプタ
301
データ処理部
303
送信データ
302
データベース
11
個人情報
サーバ30(携帯電話会社10)
102

FIG. 58

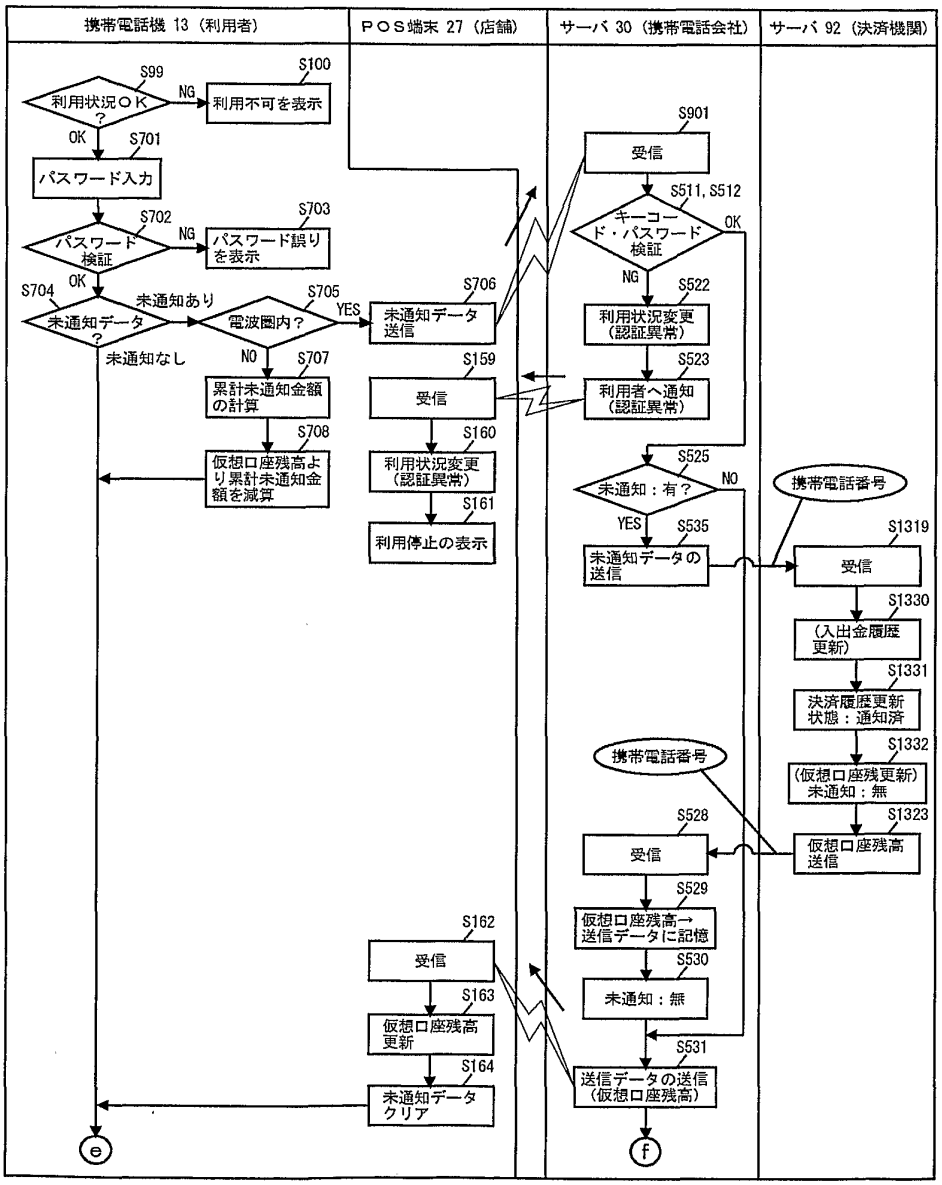

携帯電話機 13（利用者）
POS端末 27（店舗）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
S99
利用状況OK？
NG
S100
利用不可を表示
OK
S701
パスワード入力
S702
パスワード検証
NG
S703
パスワード誤りを表示
OK
S704
未通知データ？
未通知あり
S705
電波圏内？
YES
S706
未通知データ送信
未通知なし
NO
S707
累計未通知金額の計算
S708
仮想口座残高より累計未通知金額を減算
S159
受信
S160
利用状況変更（認証異常）
S161
利用停止の表示
S162
受信
S163
仮想口座残高更新
S164
未通知データクリア
S901
受信
S511, S512
キーコード・パスワード検証
OK
NG
S522
利用状況変更（認証異常）
S523
利用者へ通知（認証異常）
S525
未通知：有？
NO
YES
S535
未通知データの送信
携帯電話番号
S528
受信
S529
仮想口座残高→送信データに記憶
S530
未通知：無
S531
送信データの送信（仮想口座残高）
携帯電話番号
S1319
受信
S1330
（入出金履歴更新）
S1331
決済履歴更新状態：通知済
S1332
（仮想口座残更新）未通知：無
S1323
仮想口座残高送信
ⓔ
ⓕ

FIG. 59

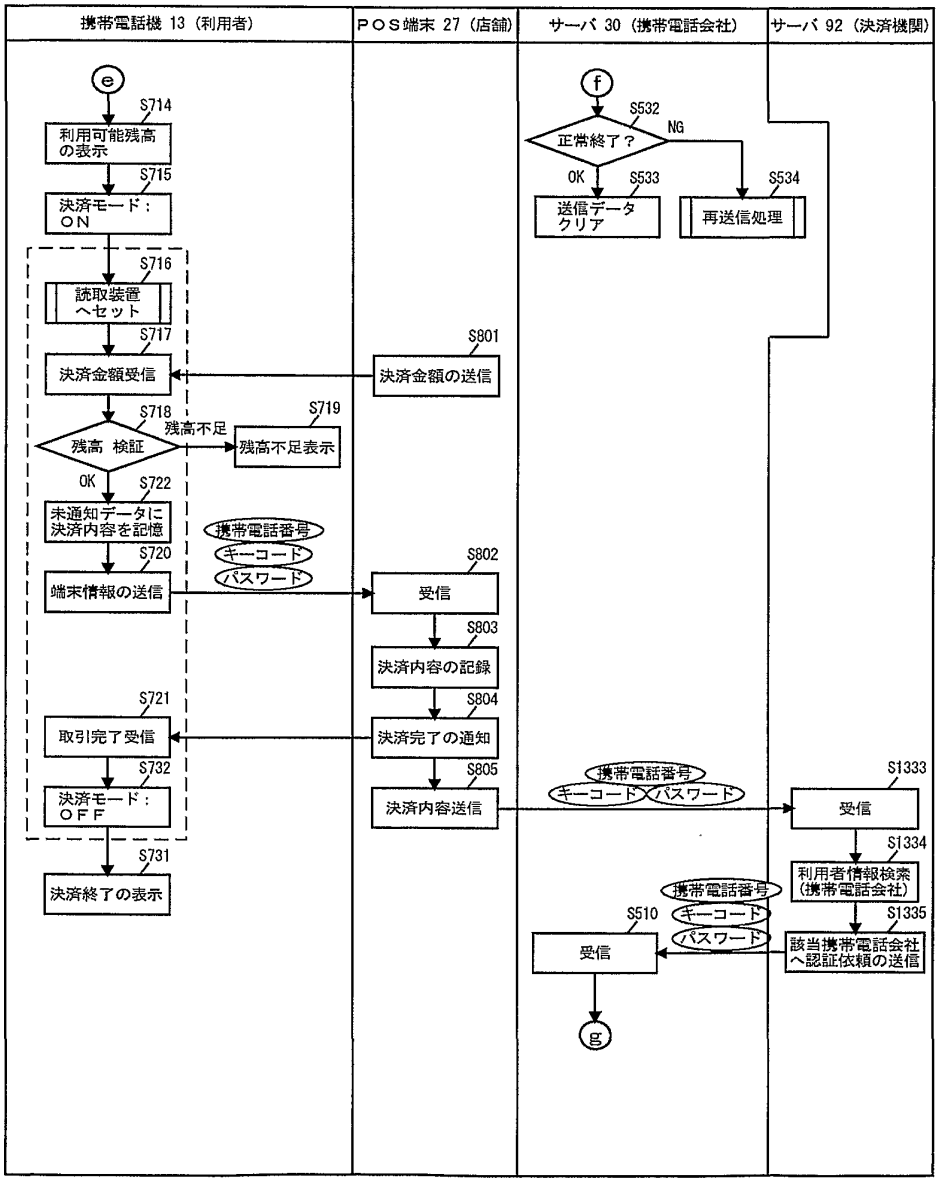

携帯電話機 13（利用者）
POS端末 27（店舗）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
e
S714
利用可能残高の表示
S715
決済モード：ON
S716
読取装置へセット
S717
決済金額受信
S718
残高 検証
残高不足
S719
残高不足表示
OK
S722
未通知データに決済内容を記憶
S720
端末情報の送信
携帯電話番号
キーコード
パスワード
S801
決済金額の送信
S802
受信
S803
決済内容の記録
S804
決済完了の通知
S805
決済内容送信
S721
取引完了受信
S732
決済モード：OFF
S731
決済終了の表示
f
S532
正常終了？
NG
OK
S533
送信データクリア
S534
再送信処理
携帯電話番号
キーコード
パスワード
S1333
受信
S1334
利用者情報検索（携帯電話会社）
携帯電話番号
キーコード
パスワード
S1335
該当携帯電話会社へ認証依頼の送信
S510
受信
g

FIG. 60

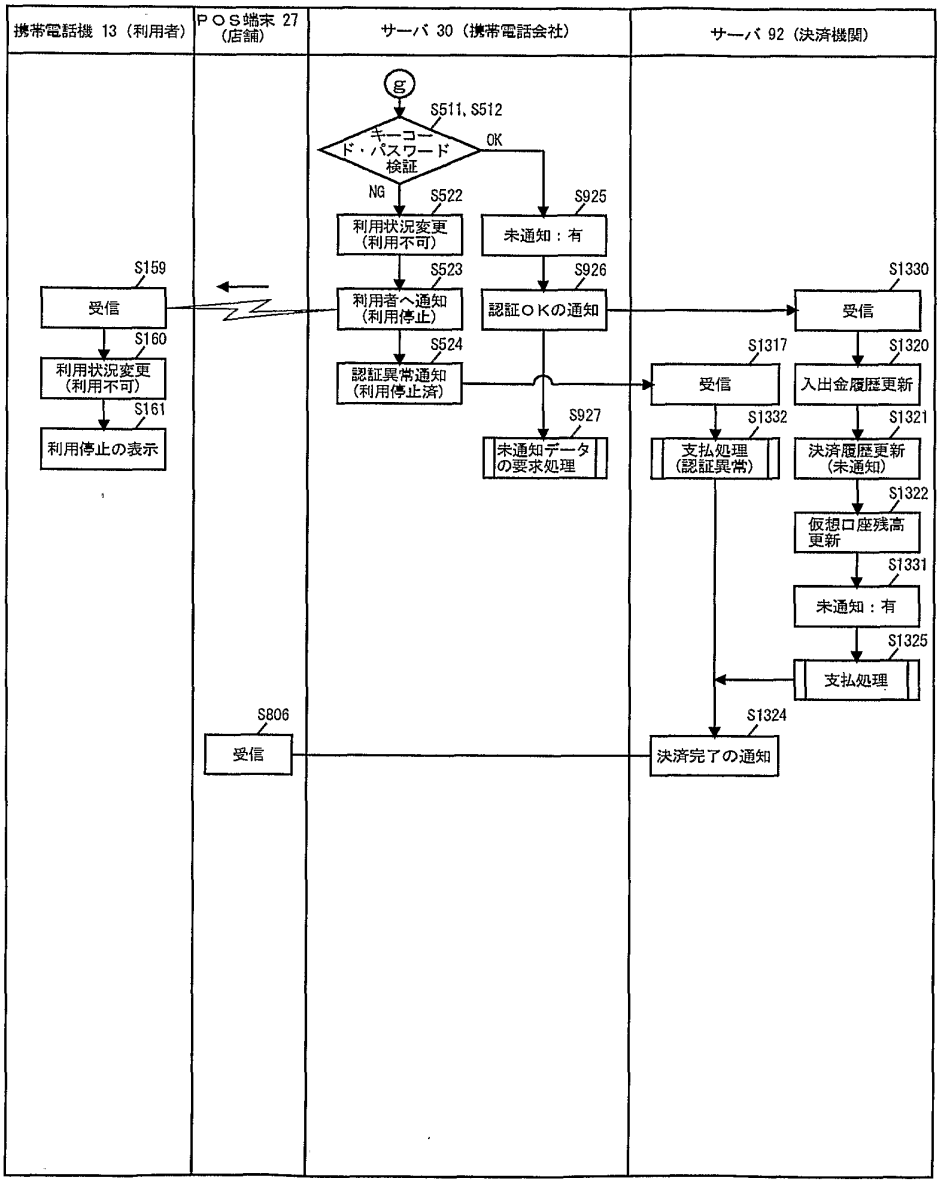

携帯電話機 13（利用者）
POS端末 27（店舗）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
g
S511、S512
キーコード・パスワード検証
OK
NG
S522
利用状況変更（利用不可）
S523
利用者へ通知（利用停止）
S524
認証異常通知（利用停止済）
S925
未通知：有
S926
認証OKの通知
S927
未通知データの要求処理
S159
受信
S160
利用状況変更（利用不可）
S161
利用停止の表示
S806
受信
S1330
受信
S1317
受信
S1320
入出金履歴更新
S1332
支払処理（認証異常）
S1321
決済履歴更新（未通知）
S1322
仮想口座残高更新
S1331
未通知：有
S1325
支払処理
S1324
決済完了の通知

FIG. 61

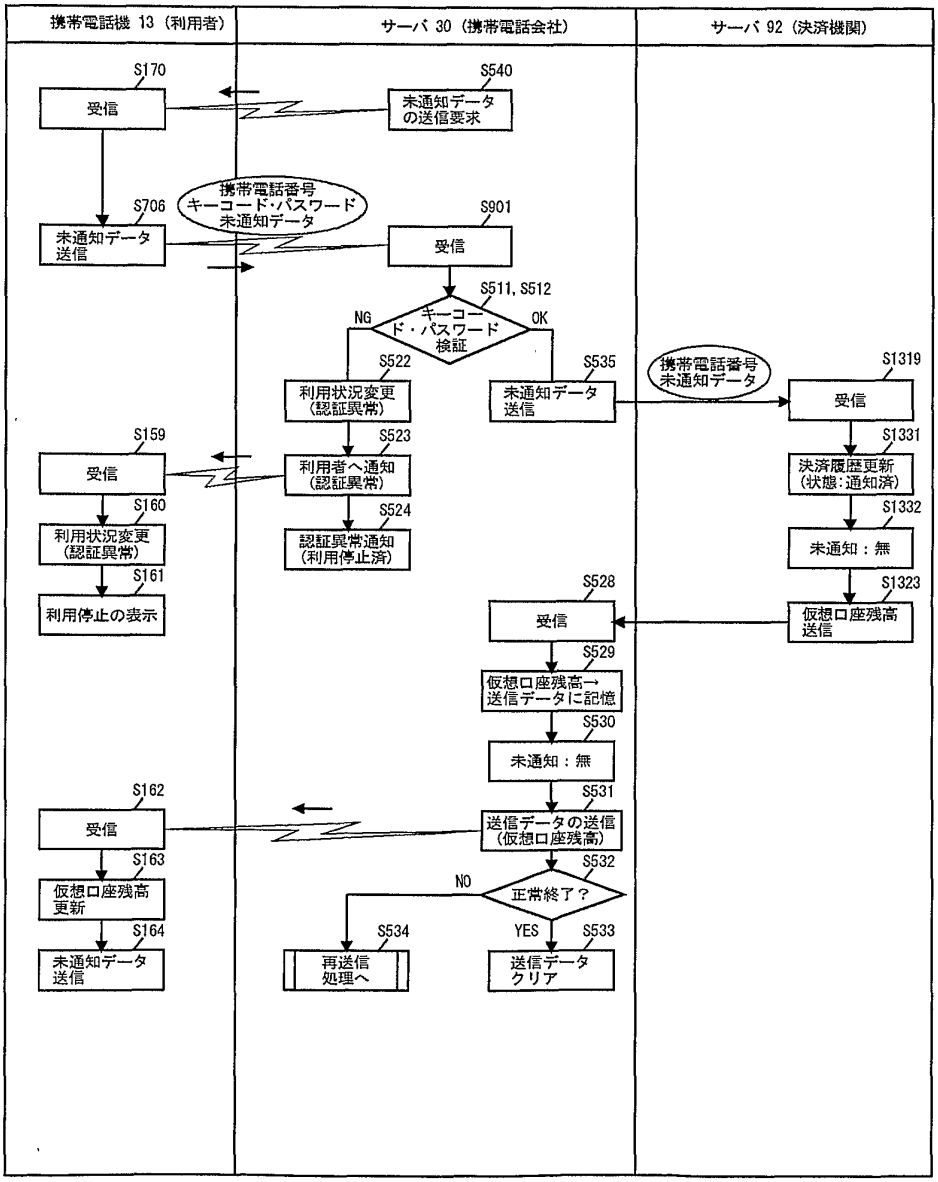
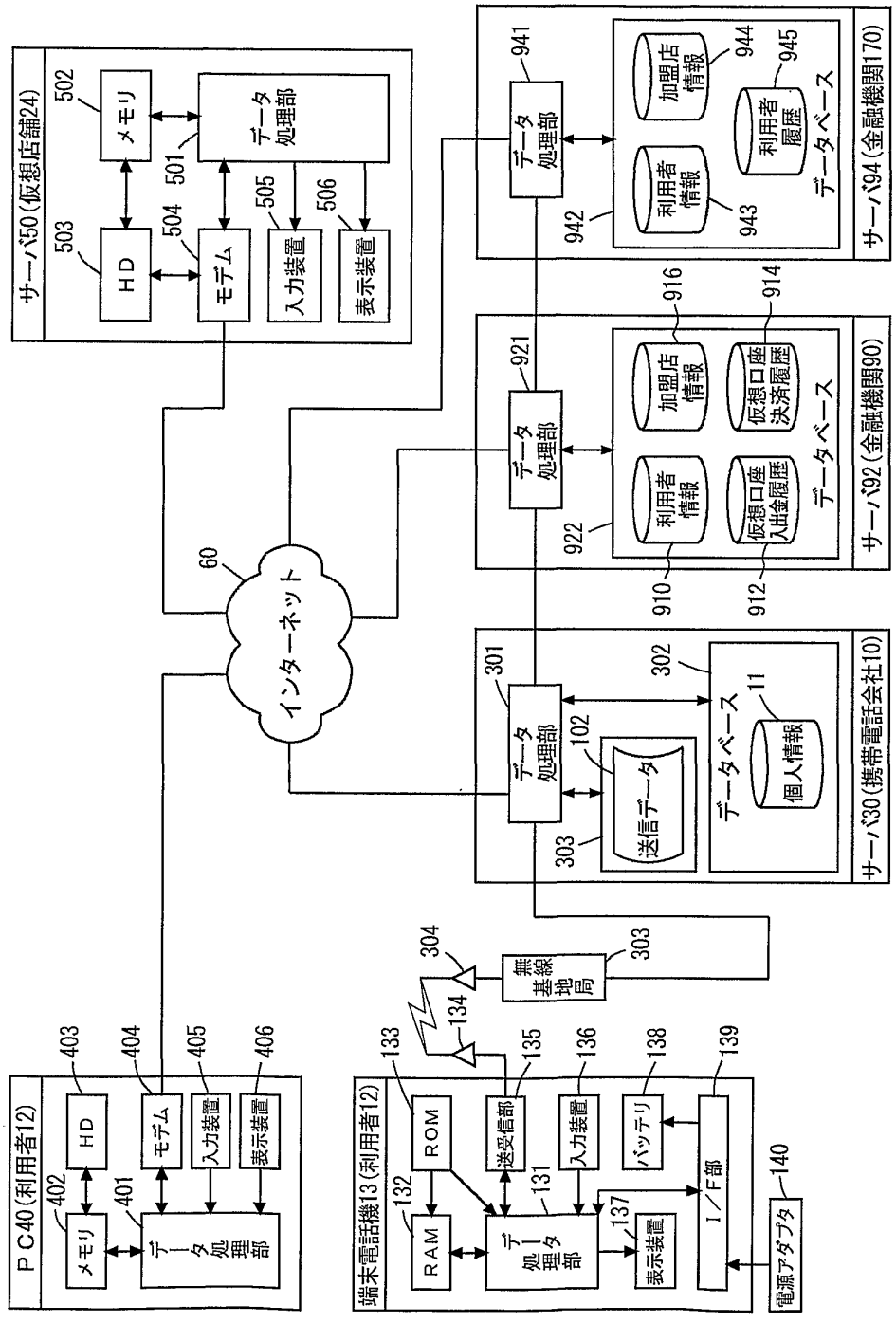

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
S170
受信
S540
未通知データの送信要求
携帯電話番号
キーコード・パスワード
未通知データ
S706
未通知データ送信
S901
受信
S511, S512
キーコード・パスワード検証
NG
OK
S522
利用状況変更（認証異常）
S535
未通知データ送信
携帯電話番号
未通知データ
S1319
受信
S159
受信
S523
利用者へ通知（認証異常）
S1331
決済履歴更新（状態：通知済）
S160
利用状況変更（認証異常）
S524
認証異常通知（利用停止済）
S1332
未通知：無
S161
利用停止の表示
S528
受信
S1323
仮想口座残高送信
S529
仮想口座残高→送信データに記憶
S530
未通知：無
S162
受信
S531
送信データの送信（仮想口座残高）
S163
仮想口座残高更新
S532
NO
正常終了？
S164
未通知データ送信
S534
再送信処理へ
YES
S533
送信データクリア

FIG. 62



APPL-1002
APPLE INC. / Page 790 of 1892

FIG. 63

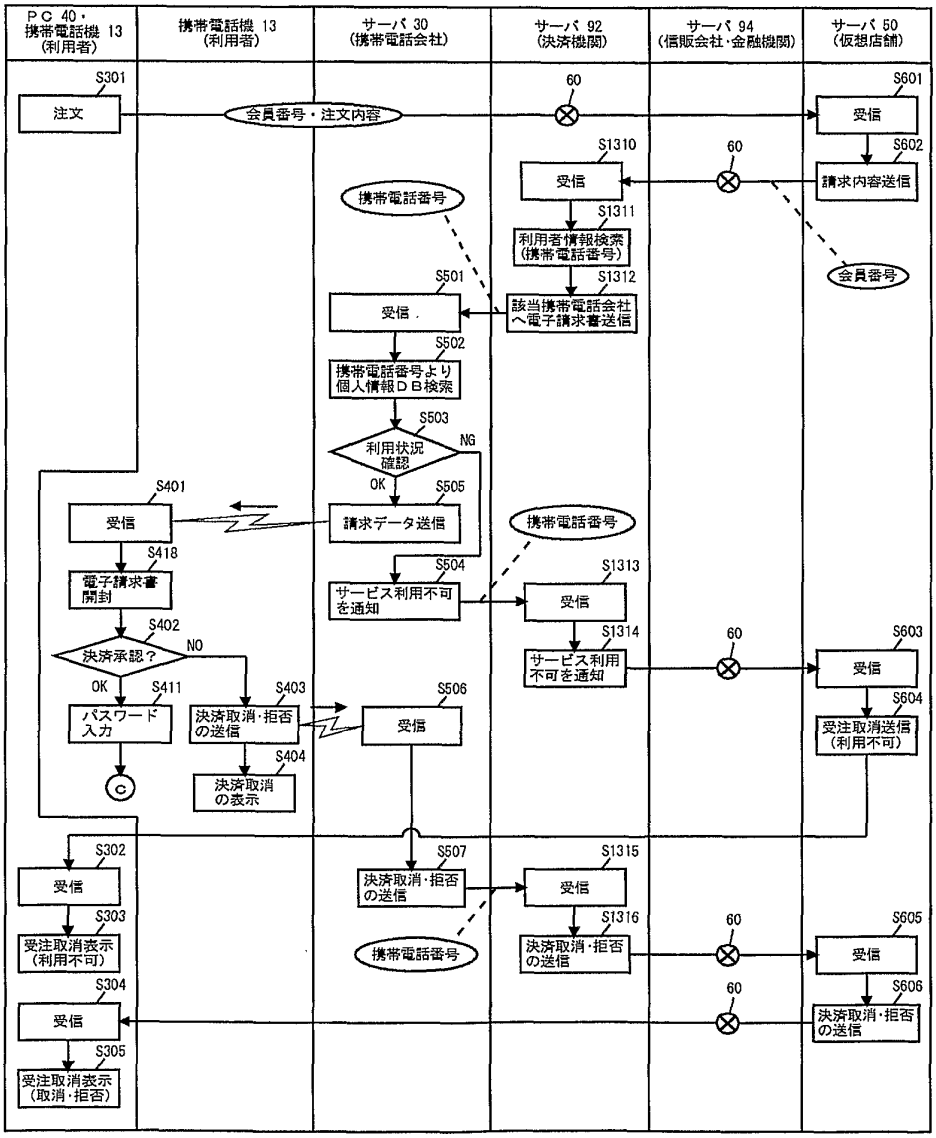

PC 40・携帯電話機 13 (利用者)
携帯電話機 13 (利用者)
サーバ 30 (携帯電話会社)
サーバ 92 (決済機関)
サーバ 94 (信販会社・金融機関)
サーバ 50 (仮想店舗)
S301
注文
会員番号・注文内容
60
S601
受信
S602
請求内容送信
S1310
受信
S1311
利用者情報検索 (携帯電話番号)
S1312
該当携帯電話会社へ電子請求書送信
携帯電話番号
会員番号
S501
受信
S502
携帯電話番号より個人情報ＤＢ検索
S503
利用状況確認
NG
OK
S505
請求データ送信
S504
サービス利用不可を通知
S1313
受信
S1314
サービス利用不可を通知
S603
受信
S604
受注取消送信 (利用不可)
S401
受信
S418
電子請求書開封
S402
決済承認？
NO
OK
S411
パスワード入力
S403
決済取消・拒否の送信
S404
決済取消の表示
S506
受信
S507
決済取消・拒否の送信
S1315
受信
S1316
決済取消・拒否の送信
S605
受信
S606
決済取消・拒否の送信
S302
受信
S303
受注取消表示 (利用不可)
S304
受信
S305
受注取消表示 (取消・拒否)

FIG. 64

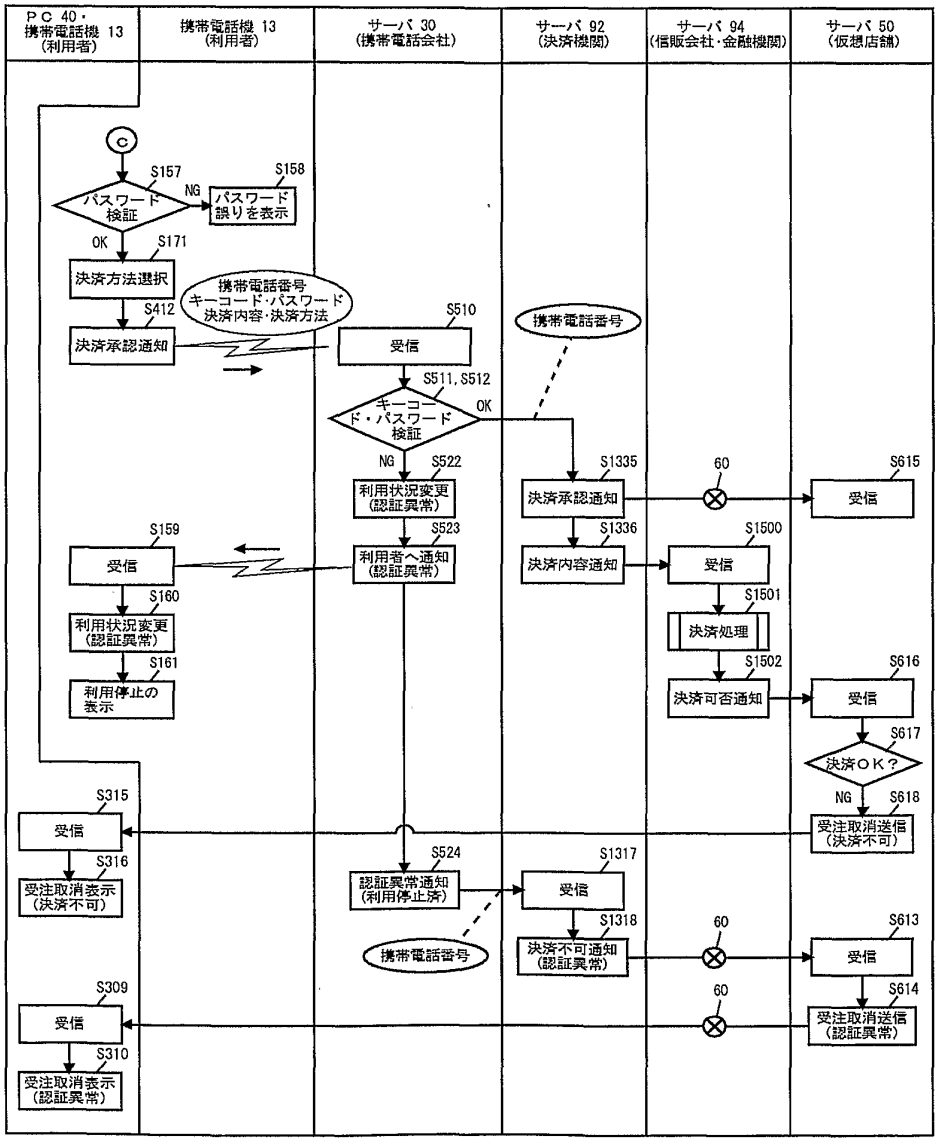

PC 40・
携帯電話機 13
(利用者)
携帯電話機 13
(利用者)
サーバ 30
(携帯電話会社)
サーバ 92
(決済機関)
サーバ 94
(信販会社・金融機関)
サーバ 50
(仮想店舗)
C
S157
パスワード検証
NG
S158
パスワード誤りを表示
OK
S171
決済方法選択
S412
決済承認通知
携帯電話番号
キーコード・パスワード
決済内容・決済方法
S510
受信
携帯電話番号
S511, S512
キーコード・パスワード検証
OK
NG
S522
利用状況変更(認証異常)
S523
利用者へ通知(認証異常)
S1335
決済承認通知
S1336
決済内容通知
60
S615
受信
S1500
受信
S1501
決済処理
S1502
決済可否通知
S616
受信
S617
決済OK?
NG
S618
受注取消送信(決済不可)
S159
受信
S160
利用状況変更(認証異常)
S161
利用停止の表示
S315
受信
S316
受注取消表示(決済不可)
S524
認証異常通知(利用停止済)
携帯電話番号
S1317
受信
S1318
決済不可通知(認証異常)
60
S613
受信
S614
受注取消送信(認証異常)
60
S309
受信
S310
受注取消表示(認証異常)

FIG. 65

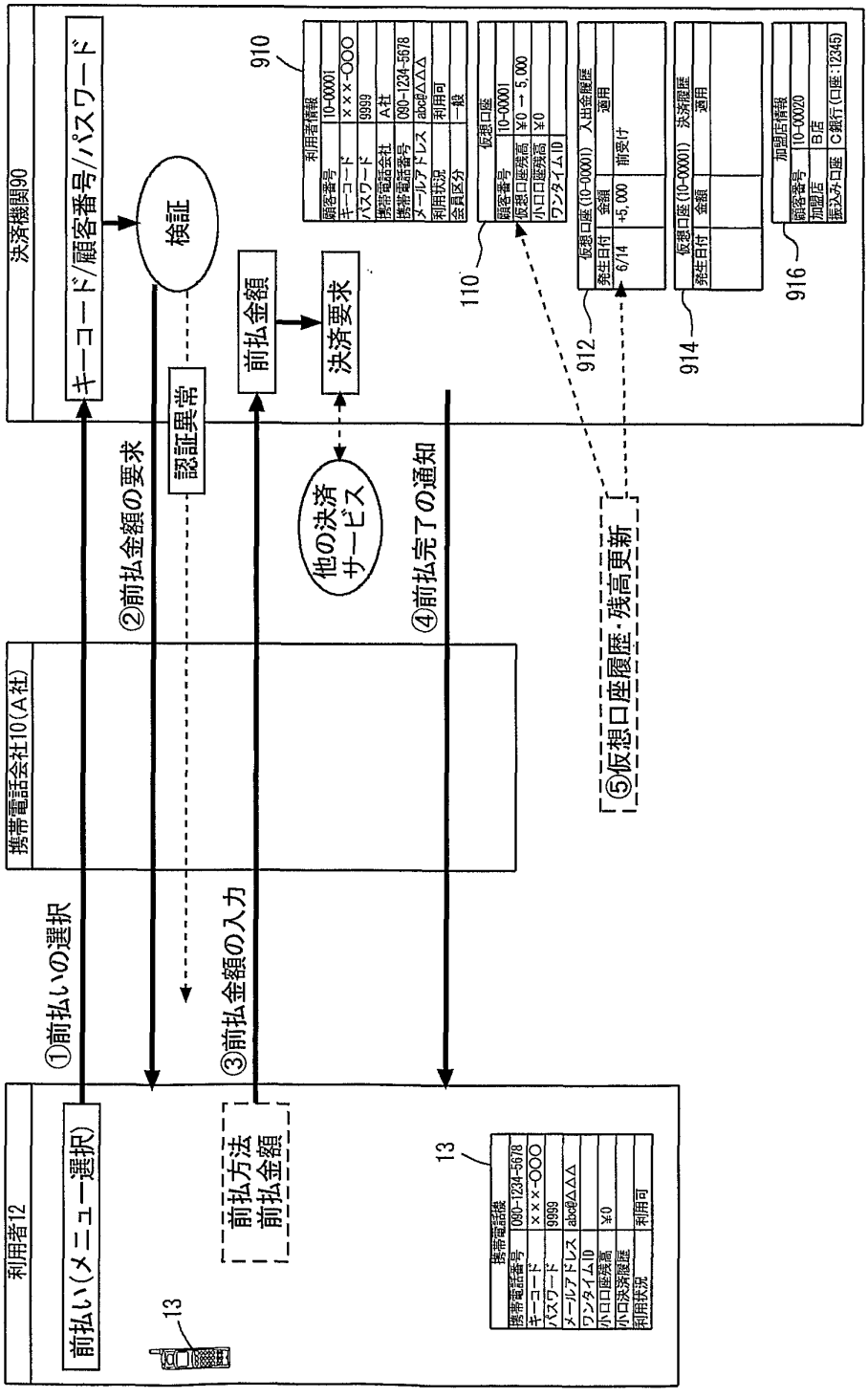

利用者12
前払い(メニュー選択)
13
前払方法
前払金額
携帯電話機
携帯電話番号 090-1234-5678
キーコード ×××-○○○
パスワード 9999
メールアドレス abc@△△△
ワンタイムID
小口座残高 ¥0
小口決済履歴
利用状況 利用可
①前払いの選択
③前払金額の入力
携帯電話会社10(A社)
決済機関90
キーコード/顧客番号/パスワード
検証
②前払金額の要求
認証異常
前払金額
決済要求
他の決済サービス
④前払完了の通知
⑤仮想口座履歴・残高更新
910
利用者情報
顧客番号 10-00001
キーコード ×××-○○○
パスワード 9999
携帯電話会社 A社
携帯電話番号 090-1234-5678
メールアドレス abc@△△△
利用状況 利用可
会員区分 一般
110
仮想口座
顧客番号 10-00001
仮想口座残高 ¥0 → 5,000
小口口座残高 ¥0
ワンタイムID
912
仮想口座(10-00001) 入出金履歴
発生日付 金額 適用
6/14 +5,000 前受け
914
仮想口座(10-00001) 決済履歴
発生日付 金額 適用
916
加盟店情報
顧客番号 10-00020
加盟店 B店
振込み口座 C銀行(口座:12345)

FIG. 66

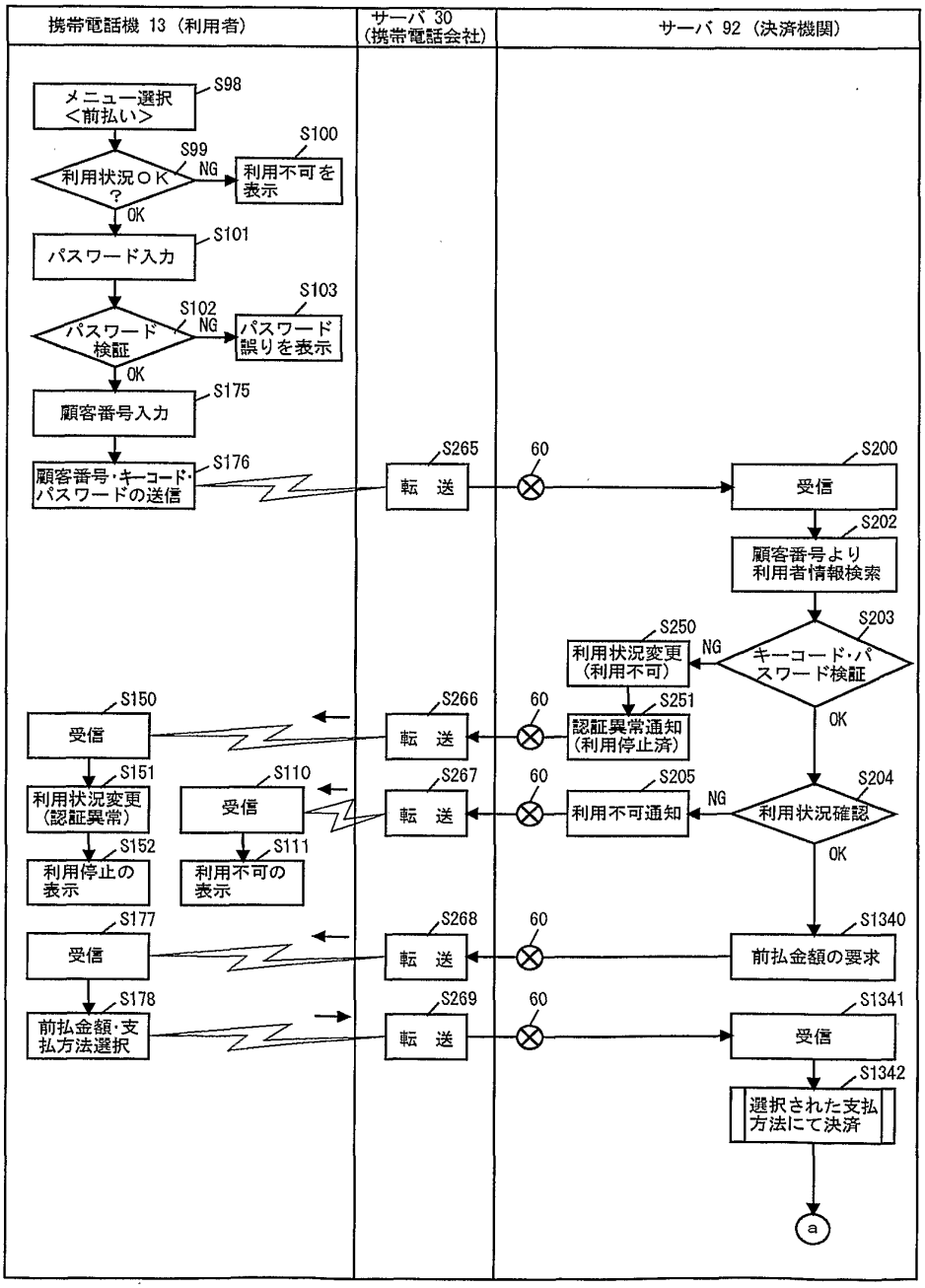

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
メニュー選択<前払い>
S98
利用状況OK？
S99
NG
S100
利用不可を表示
OK
パスワード入力
S101
パスワード検証
S102
NG
S103
パスワード誤りを表示
OK
顧客番号入力
S175
顧客番号・キーコード・パスワードの送信
S176
S265
転送
60
S200
受信
S202
顧客番号より利用者情報検索
S203
キーコード・パスワード検証
NG
S250
利用状況変更（利用不可）
S251
認証異常通知（利用停止済）
OK
S204
利用状況確認
NG
S205
利用不可通知
S267
S266
S150
受信
S151
利用状況変更（認証異常）
S152
利用停止の表示
S110
受信
S111
利用不可の表示
OK
S1340
前払金額の要求
S268
S177
受信
S178
前払金額・支払方法選択
S269
S1341
受信
S1342
選択された支払方法にて決済
a

FIG. 67

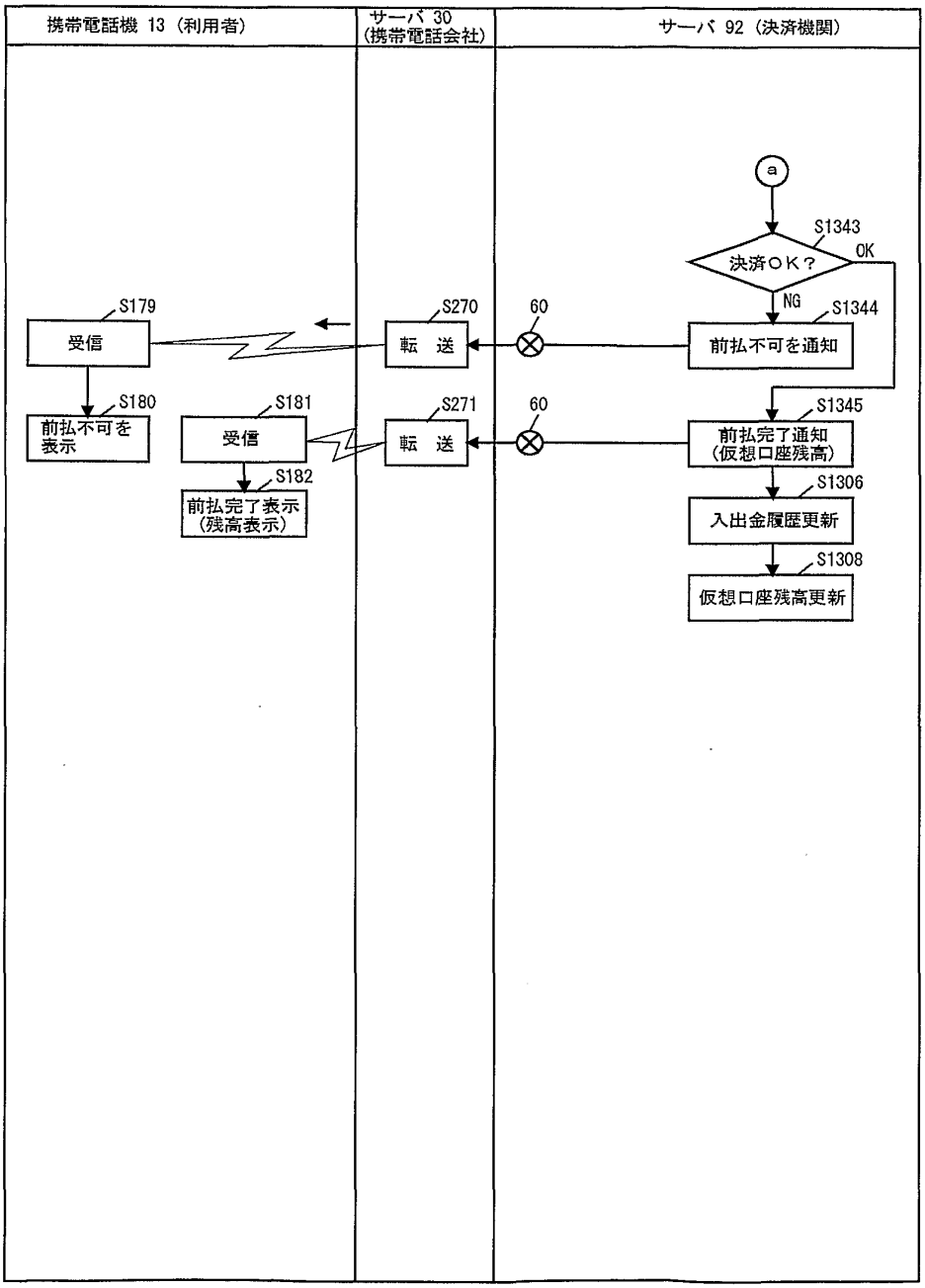

携帯電話機 13（利用者）
サーバ 30
（携帯電話会社）
サーバ 92（決済機関）
a
S1343
決済ＯＫ？
OK
NG
S1344
前払不可を通知
60
S270
転　送
S179
受信
S180
前払不可を表示
S181
受信
S271
転　送
60
S182
前払完了表示
（残高表示）
S1345
前払完了通知
（仮想口座残高）
S1306
入出金履歴更新
S1308
仮想口座残高更新

FIG. 68

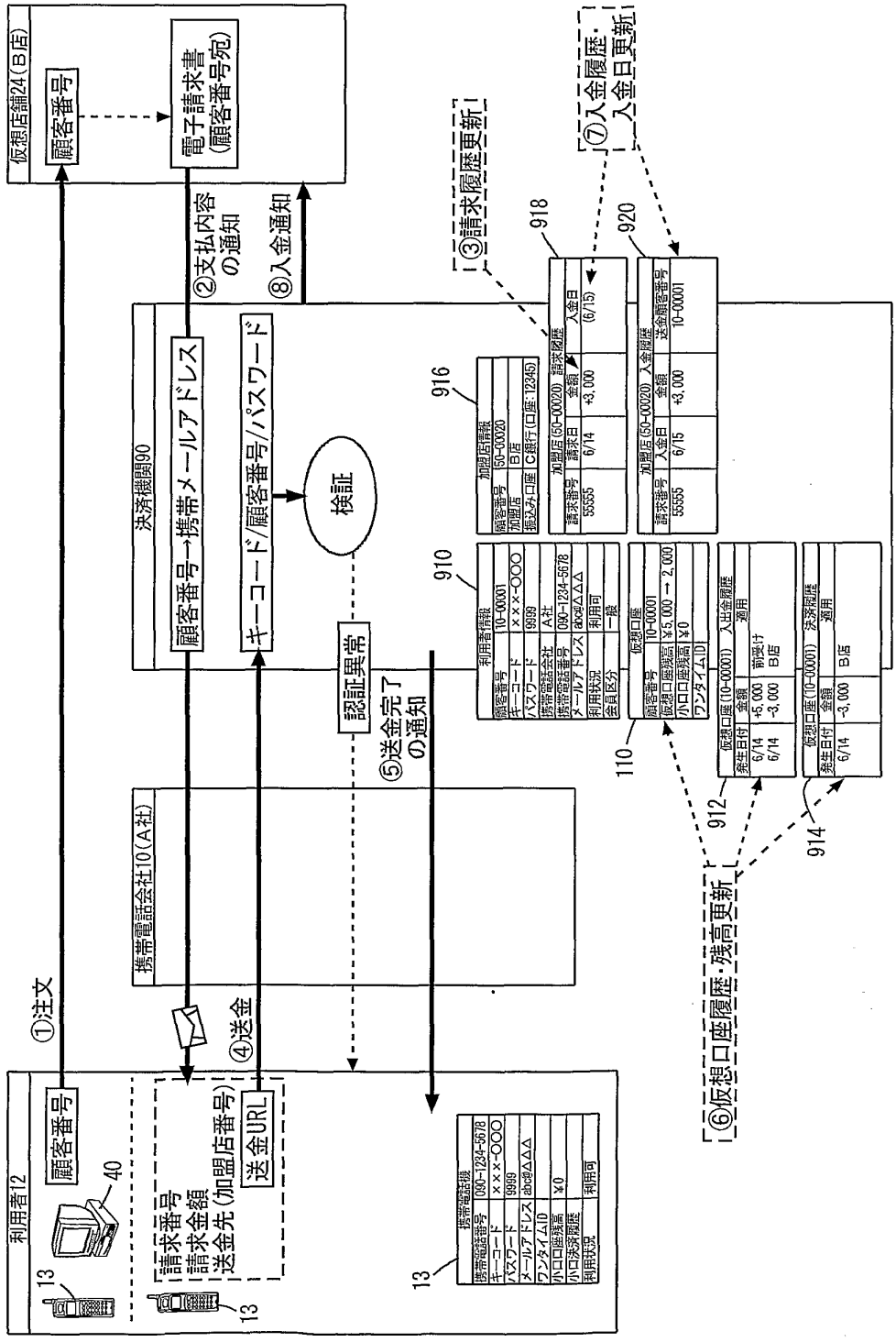

仮想店舗24(B店)
顧客番号
電子請求書(顧客番号宛)
②支払内容の通知
⑧入金通知
決済機関90
顧客番号→携帯メールアドレス
キーコード/顧客番号/パスワード
検証
認証異常
⑤送金完了の通知
携帯電話会社10(A社)
①注文
④送金
利用者12
顧客番号
送金URL
請求番号
請求金額
送金先(加盟店番号)
③請求履歴更新
⑦入金履歴・入金日更新
⑥仮想口座履歴・残高更新
910
916
918
920
912
914
110
13
40

FIG. 69

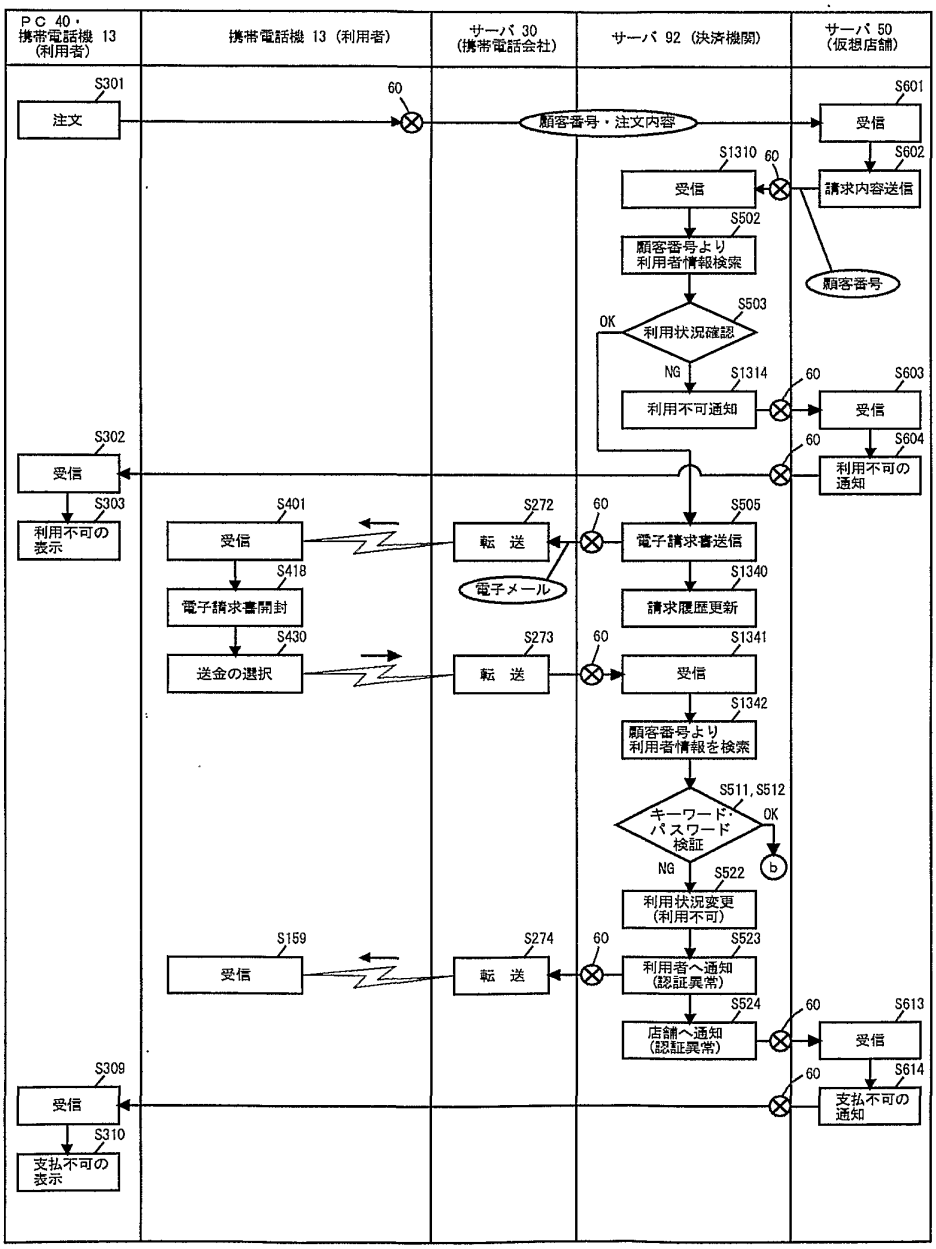

PC 40・携帯電話機 13（利用者）
携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
サーバ 50（仮想店舗）
S301
注文
60
顧客番号・注文内容
S601
受信
S602
請求内容送信
顧客番号
S1310
受信
S502
顧客番号より利用者情報検索
S503
利用状況確認
OK
NG
S1314
利用不可通知
S603
受信
S604
利用不可の通知
S302
受信
S303
利用不可の表示
S401
受信
S418
電子請求書開封
S430
送金の選択
S272
転 送
電子メール
S273
転 送
S505
電子請求書送信
S1340
請求履歴更新
S1341
受信
S1342
顧客番号より利用者情報を検索
S511, S512
キーワード・パスワード検証
OK
NG
b
S522
利用状況変更（利用不可）
S523
利用者へ通知（認証異常）
S524
店舗へ通知（認証異常）
S159
受信
S274
転 送
S613
受信
S614
支払不可の通知
S309
受信
S310
支払不可の表示

FIG. 70

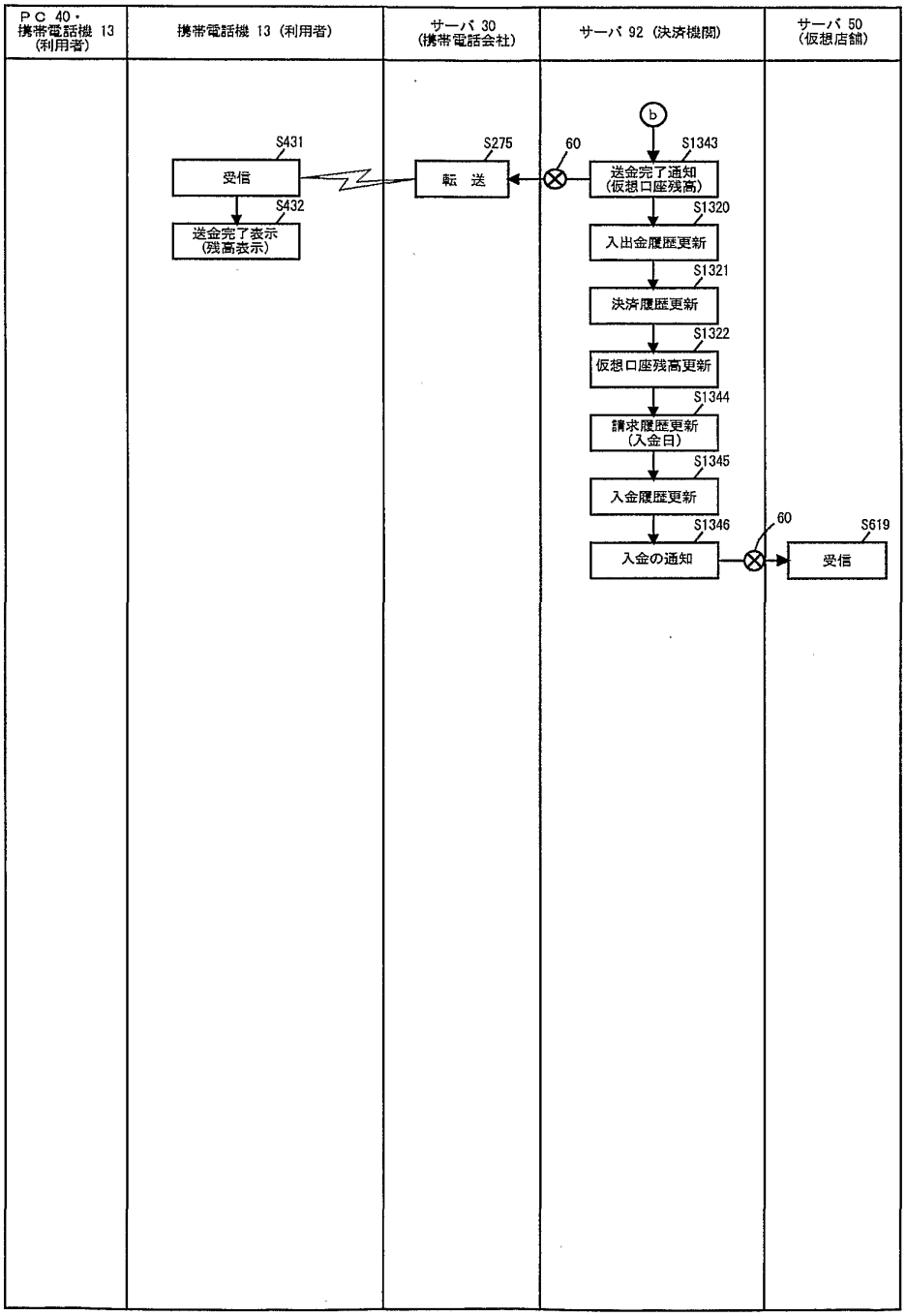

PC 40・
携帯電話機 13
(利用者)
携帯電話機 13 (利用者)
サーバ 30
(携帯電話会社)
サーバ 92 (決済機関)
サーバ 50
(仮想店舗)
b
S431
受信
S432
送金完了表示
(残高表示)
S275
転 送
60
S1343
送金完了通知
(仮想口座残高)
S1320
入出金履歴更新
S1321
決済履歴更新
S1322
仮想口座残高更新
S1344
請求履歴更新
(入金日)
S1345
入金履歴更新
S1346
入金の通知
60
S619
受信

FIG. 71

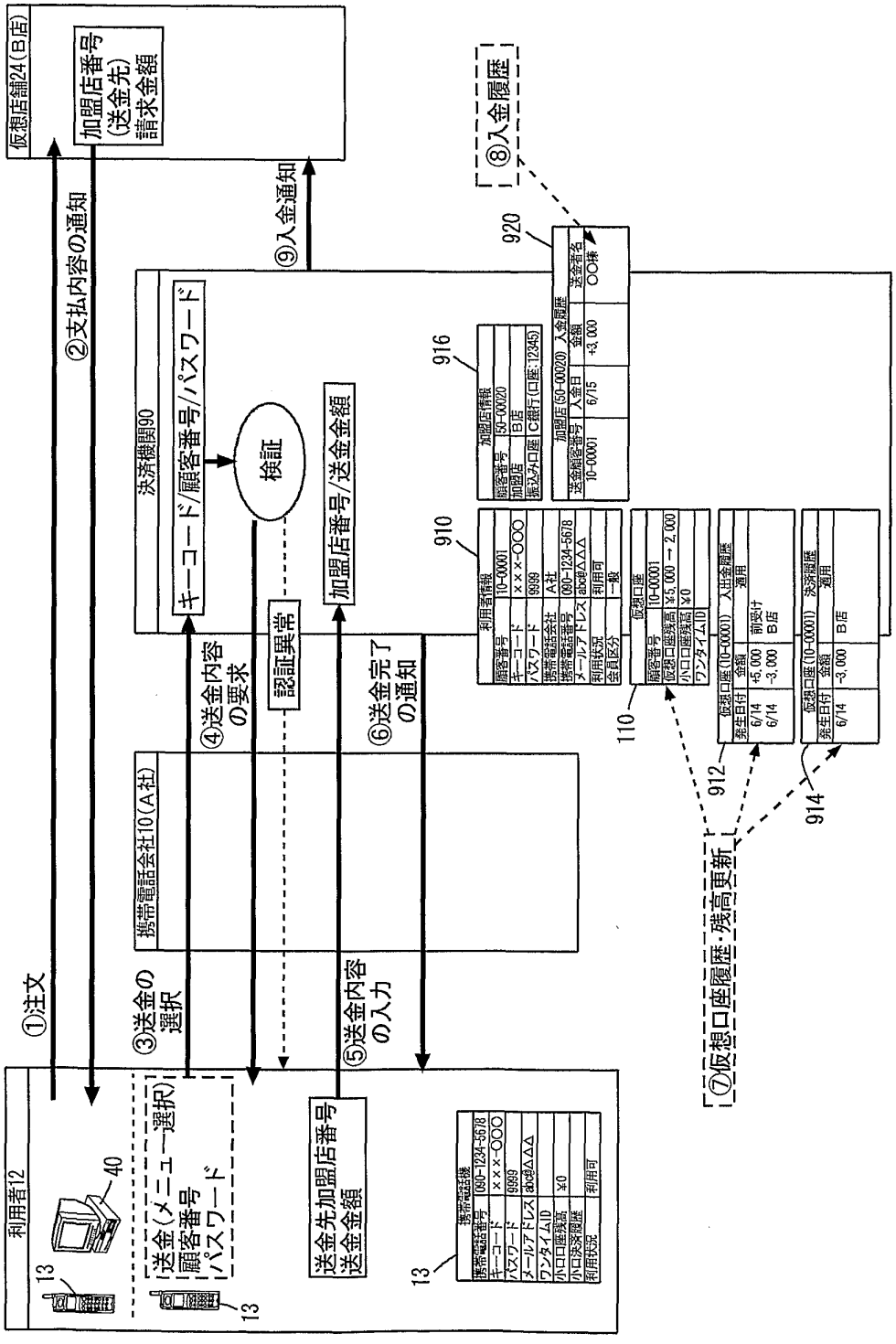

仮想店舗24(B店)
加盟店番号
(送金先)
請求金額
②支払内容の通知
⑨入金通知
⑧入金履歴
920
決済機関90
キーコード/顧客番号/パスワード
検証
916
910
加盟店番号/送金金額
認証異常
④送金内容
の要求
⑥送金完了
の通知
携帯電話会社10(A社)
③送金の
選択
①注文
利用者12
40
13
「送金(メニュー選択)
顧客番号
パスワード」
送金先加盟店番号
送金金額
⑤送金内容
の入力
携帯電話機
携帯電話番号 080-1234-5678
キーコード ×××-OOO
パスワード 9999
メールアドレス abc@△△△
ワンタイムID
小口口座残高 ¥0
小口決済履歴
利用状況 利用可
利用者情報
顧客番号 10-00001
キーコード ×××-OOO
パスワード 9999
携帯電話会社 A社
携帯電話番号 080-1234-5678
メールアドレス abc@△△△
利用状況 利用可
会員区分 一般
加盟店情報
顧客番号 50-00020
加盟店 B店
振込み口座 C銀行(口座:12345)
送金顧客番号 入金日 金額 送金者名
10-00001 6/15 +3,000 OO様
仮想口座
顧客番号 10-00001
仮想口座残高 ¥5,000 → 2,000
小口口座残高 ¥0
ワンタイムID
仮想口座(10-00001) 入出金履歴
発生日付 金額 適用
6/14 +5,000 前受け
6/14 -3,000 B店
仮想口座(10-00001) 決済履歴
発生日付 金額 適用
6/14 -3,000 B店
110
912
914
「⑦仮想口座履歴・残高更新」

FIG. 72

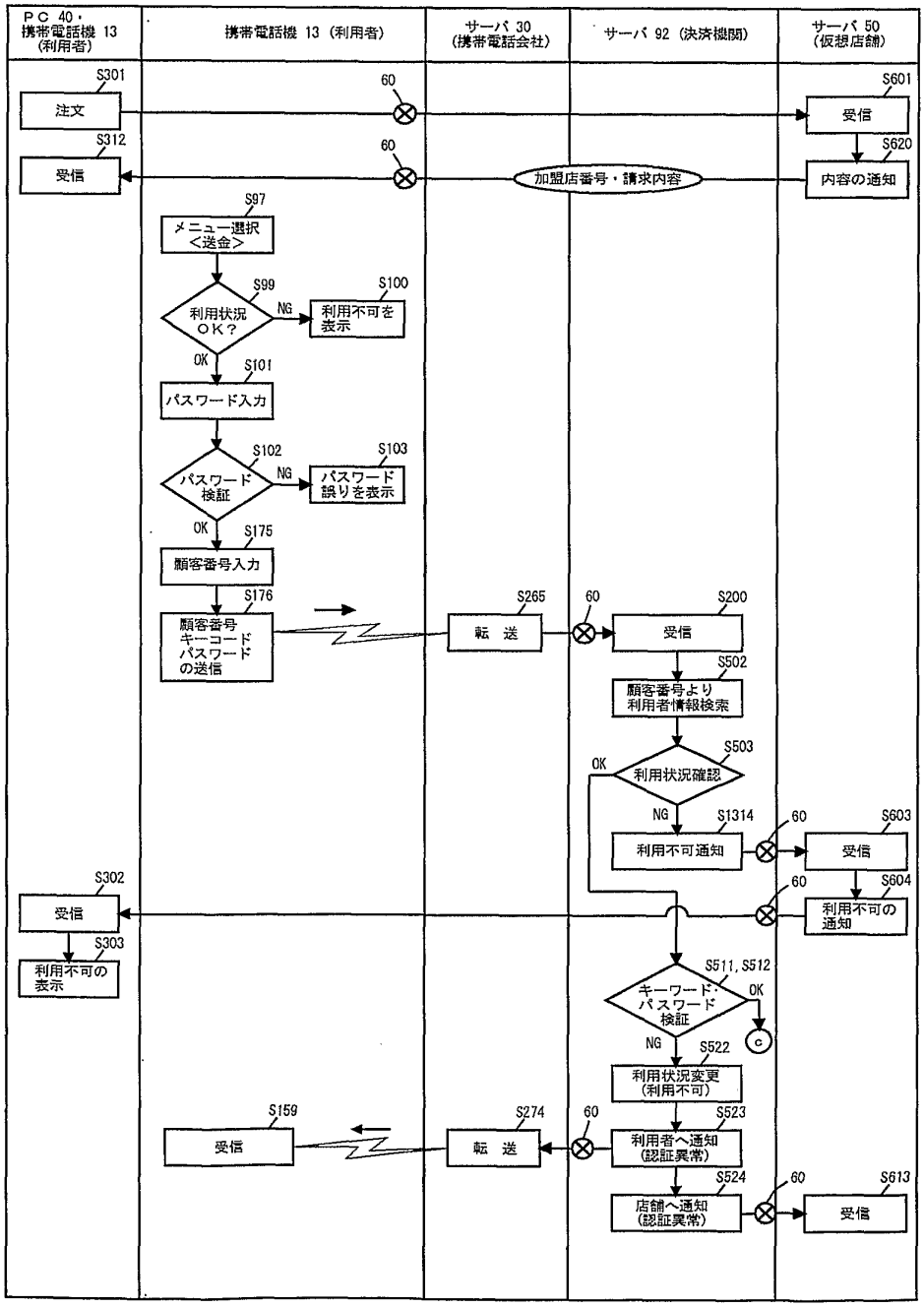

PC 40・
携帯電話機 13
(利用者)
携帯電話機 13 (利用者)
サーバ 30
(携帯電話会社)
サーバ 92 (決済機関)
サーバ 50
(仮想店舗)
S301
注文
60
S601
受信
S312
受信
60
加盟店番号・請求内容
S620
内容の通知
S97
メニュー選択
<送金>
S99
利用状況
OK?
NG
S100
利用不可を
表示
OK
S101
パスワード入力
S102
パスワード
検証
NG
S103
パスワード
誤りを表示
OK
S175
顧客番号入力
S176
顧客番号
キーコード
パスワード
の送信
S265
転 送
60
S200
受信
S502
顧客番号より
利用者情報検索
S503
OK
利用状況確認
NG
S1314
利用不可通知
60
S603
受信
S302
受信
60
S604
利用不可の
通知
S303
利用不可の
表示
S511, S512
キーワード・
パスワード
検証
OK
NG
S522
利用状況変更
(利用不可)
S159
受信
S274
転 送
60
S523
利用者へ通知
(認証異常)
S524
店舗へ通知
(認証異常)
60
S613
受信

FIG. 73

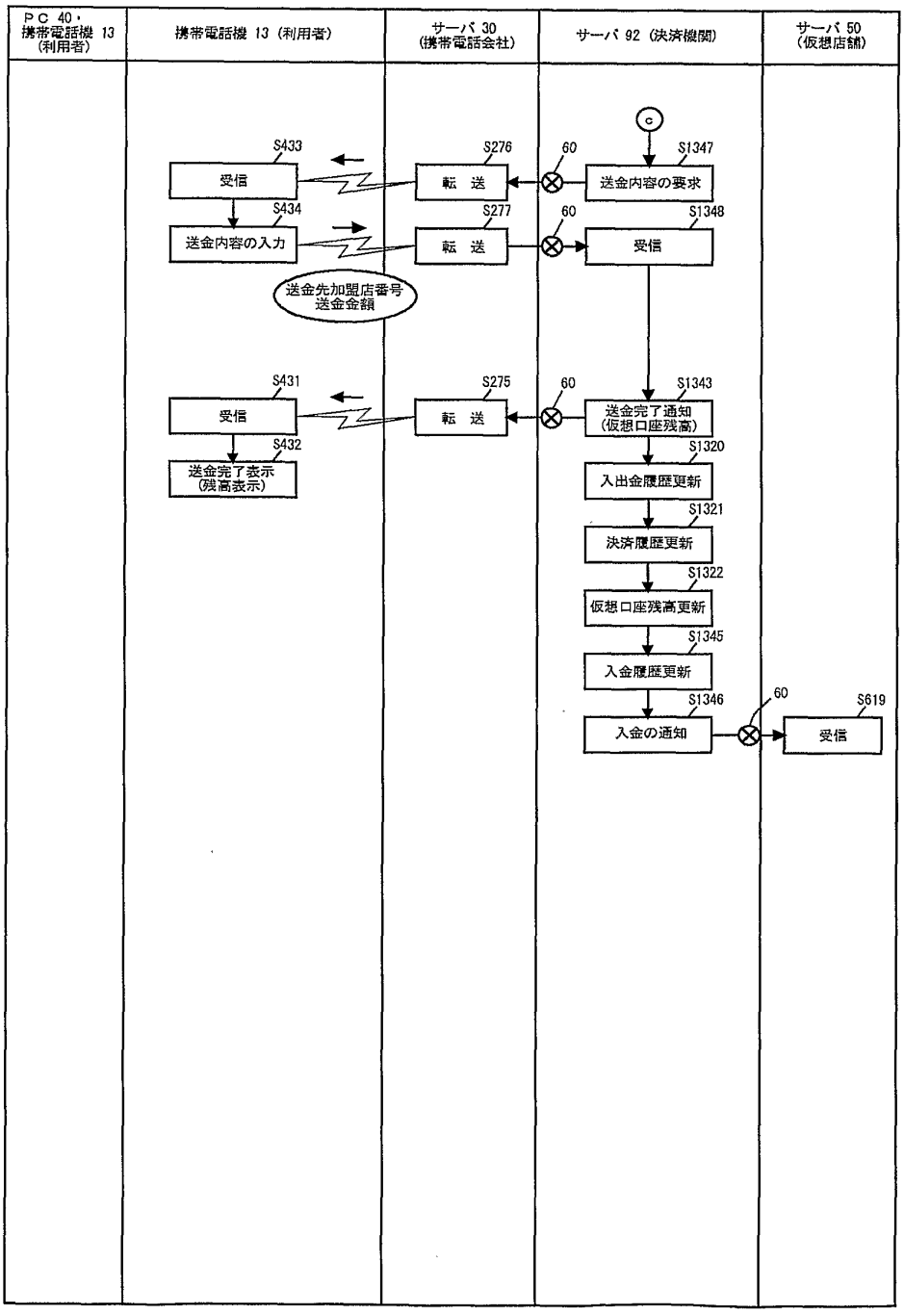

PC 40・携帯電話機 13 (利用者)
携帯電話機 13 (利用者)
サーバ 30 (携帯電話会社)
サーバ 92 (決済機関)
サーバ 50 (仮想店舗)
C
S433
受信
S434
送金内容の入力
送金先加盟店番号
送金金額
S276
転 送
S277
転 送
60
S1347
送金内容の要求
S1348
受信
S431
受信
S432
送金完了表示 (残高表示)
S275
転 送
S1343
送金完了通知 (仮想口座残高)
S1320
入出金履歴更新
S1321
決済履歴更新
S1322
仮想口座残高更新
S1345
入金履歴更新
S1346
入金の通知
S619
受信

FIG. 74

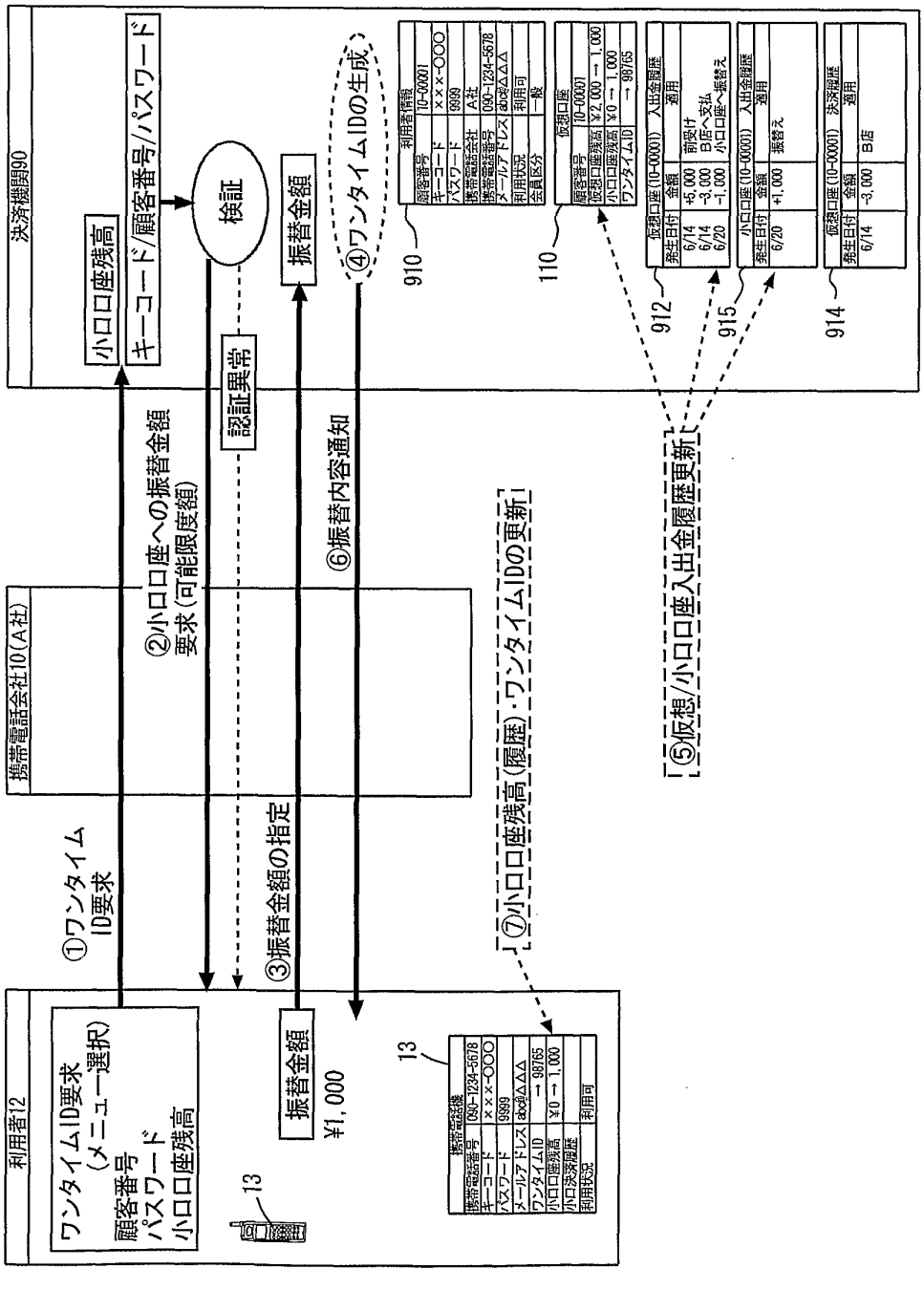

利用者12
ワンタイムID要求
(メニュー選択)
顧客番号
パスワード
小口口座残高
振替金額
¥1,000
13
携帯電話番号 090-1234-5678
キーコード ×××-○○○
パスワード 9999
メールアドレス abc@△△△
ワンタイムID → 98765
小口口座残高 ¥0 → 1,000
小口決済履歴
利用状況 利用可
携帯電話会社10(A社)
①ワンタイムID要求
②小口口座への振替金額要求(可能限度額)
③振替金額の指定
⑥振替内容通知
「⑦小口口座残高(履歴)・ワンタイムIDの更新」
決済機関90
小口口座残高
キーコード/顧客番号/パスワード
検証
認証異常
振替金額
④ワンタイムIDの生成
910
利用者情報
顧客番号 10-00001
キーコード ×××-○○○
パスワード 9999
携帯電話会社 A社
携帯電話番号 090-1234-5678
メールアドレス abc@△△△
利用状況 利用可
会員区分 一般
110
仮想口座
顧客番号 10-00001
仮想口座残高 ¥2,000 → 1,000
小口口座残高 ¥0 → 1,000
ワンタイムID → 98765
「⑤仮想/小口口座入出金履歴更新」
912
仮想口座(10-00001) 入出金履歴
発生日付 金額 適用
6/14 +5,000 前受け
6/14 -3,000 B店へ支払
6/20 -1,000 小口口座へ振替え
915
小口口座(10-00001) 入出金履歴
発生日付 金額 適用
6/20 +1,000 振替え
914
仮想口座(10-00001) 決済履歴
発生日付 金額 適用
6/14 -3,000 B店

FIG. 75

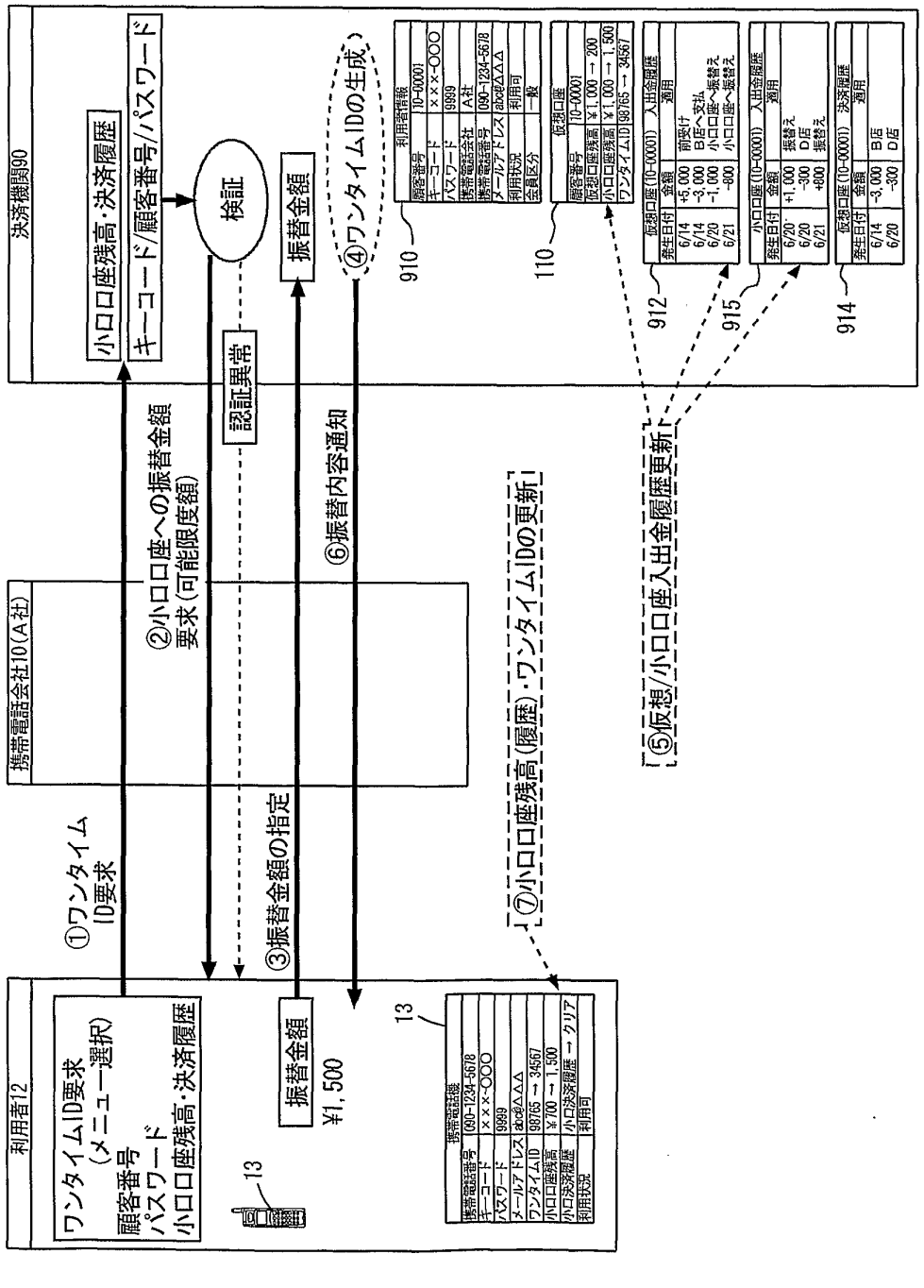

決済機関90
小口口座残高・決済履歴
キーコード/顧客番号/パスワード
検証
認証異常
振替金額
④ワンタイムIDの生成
利用者情報
顧客番号 10-00001
キーコード ×××-OOO
パスワード 9999
携帯電話会社 A社
携帯電話番号 090-1234-5678
メールアドレス abcde△△△
利用状況 利用可
会員区分 一般
910
仮想口座
顧客番号 10-00001
仮想口座残高 ¥1,000 → 200
小口口座残高 ¥1,000 → 1,500
ワンタイムID 98765 → 34567
110
仮想口座(10-00001) 入出金履歴
発生日付 金額 適用
6/14 +5,000 前受け
6/14 -3,000 B店へ支払
6/20 -1,000 小口口座へ振替え
6/21 -600 小口口座へ返替え
912
小口口座(10-00001) 入出金履歴
発生日付 金額 適用
6/20 +1,000 振替え
6/20 -300 D店
6/21 +600 振替え
915
仮想口座(10-00001) 決済履歴
発生日付 金額 適用
6/14 -3,000 B店
6/20 -300 D店
914
⑤仮想/小口口座入出金履歴更新
⑦小口口座残高(履歴)・ワンタイムIDの更新
⑥振替内容通知
①ワンタイムID要求
②小口口座への振替金額要求(可能限度額)
③振替金額の指定
携帯電話会社10(A社)
利用者12
ワンタイムID要求
(メニュー選択)
顧客番号
パスワード
小口口座残高・決済履歴
振替金額
¥1,500
13
携帯電話端末
携帯電話番号 090-1234-5678
キーコード ×××-OOO
パスワード 9999
メールアドレス abcde△△△
ワンタイムID 98765 → 34567
小口口座残高 ¥700 → 1,500
小口決済履歴 小口決済履歴 → クリア
利用状況 利用可

FIG. 76

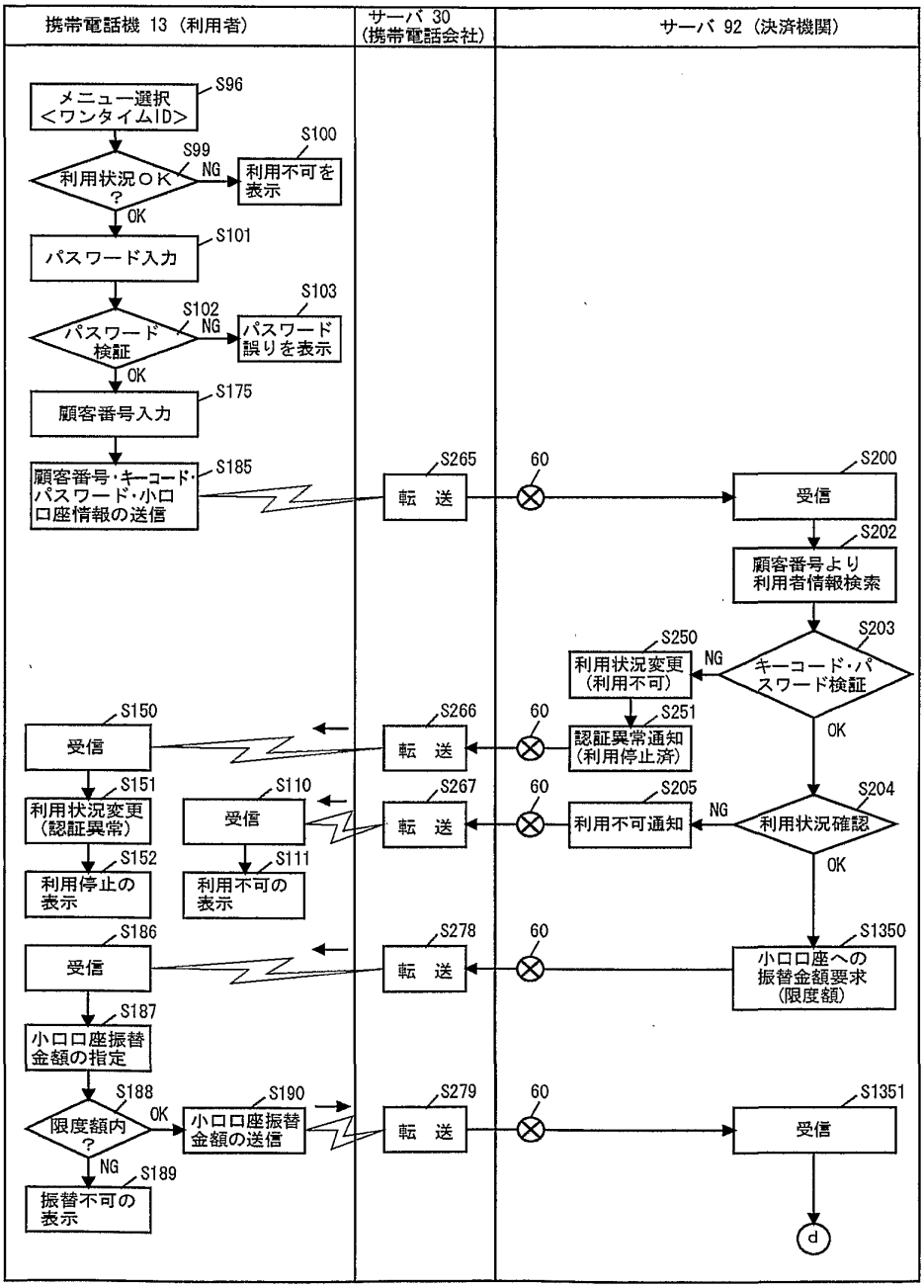

携帯電話機 13（利用者）
サーバ 30（携帯電話会社）
サーバ 92（決済機関）
メニュー選択 <ワンタイムID>
S96
利用状況ＯＫ？
S99
NG
S100
利用不可を表示
OK
パスワード入力
S101
パスワード検証
S102
NG
S103
パスワード誤りを表示
OK
顧客番号入力
S175
顧客番号・キーコード・パスワード・小口口座情報の送信
S185
転 送
S265
60
受信
S200
顧客番号より利用者情報検索
S202
キーコード・パスワード検証
S203
NG
利用状況変更（利用不可）
S250
認証異常通知（利用停止済）
S251
OK
利用状況確認
S204
NG
利用不可通知
S205
OK
小口口座への振替金額要求（限度額）
S1350
受信
S1351
d
受信
S150
転 送
S266
利用状況変更（認証異常）
S151
受信
S110
転 送
S267
利用停止の表示
S152
利用不可の表示
S111
受信
S186
転 送
S278
小口口座振替金額の指定
S187
限度額内？
S188
OK
小口口座振替金額の送信
S190
転 送
S279
NG
振替不可の表示
S189

FIG. 77

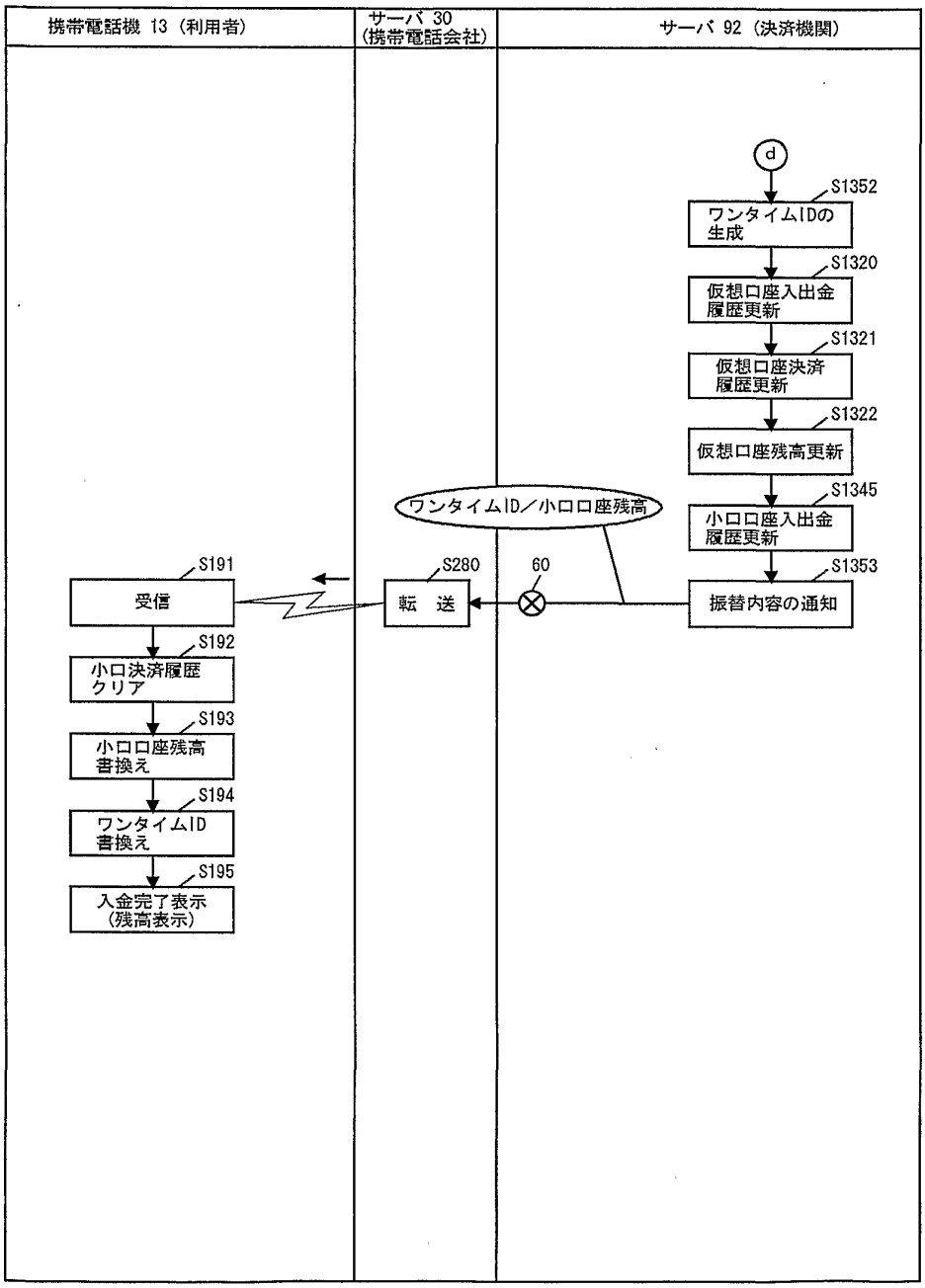

携帯電話機 13（利用者）
サーバ 30
（携帯電話会社）
サーバ 92（決済機関）
d
S1352
ワンタイムIDの生成
S1320
仮想口座入出金履歴更新
S1321
仮想口座決済履歴更新
S1322
仮想口座残高更新
S1345
小口口座入出金履歴更新
S1353
振替内容の通知
ワンタイムID／小口口座残高
60
S280
転　送
S191
受信
S192
小口決済履歴クリア
S193
小口口座残高書換え
S194
ワンタイムID書換え
S195
入金完了表示（残高表示）

FIG. 78

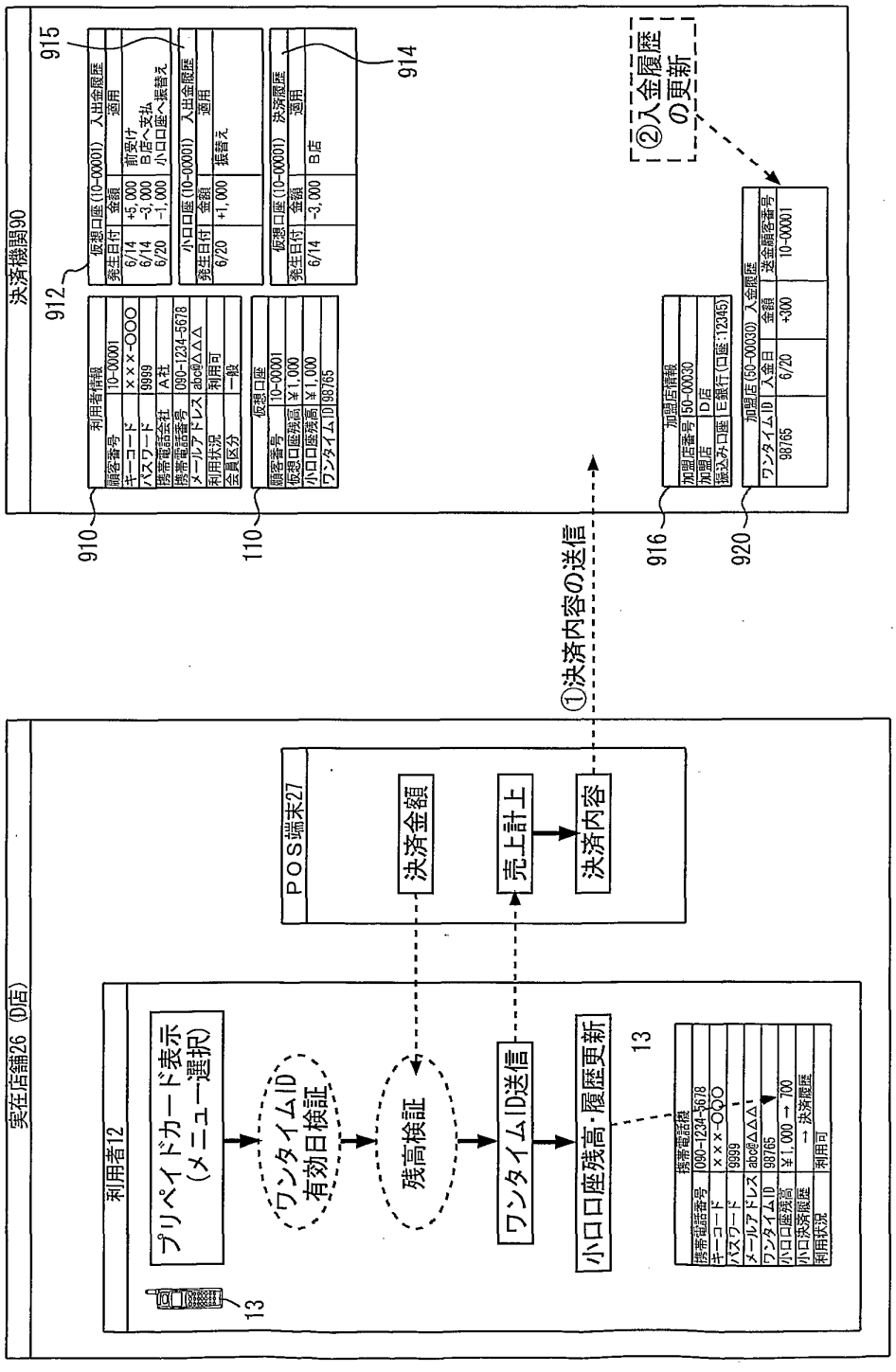
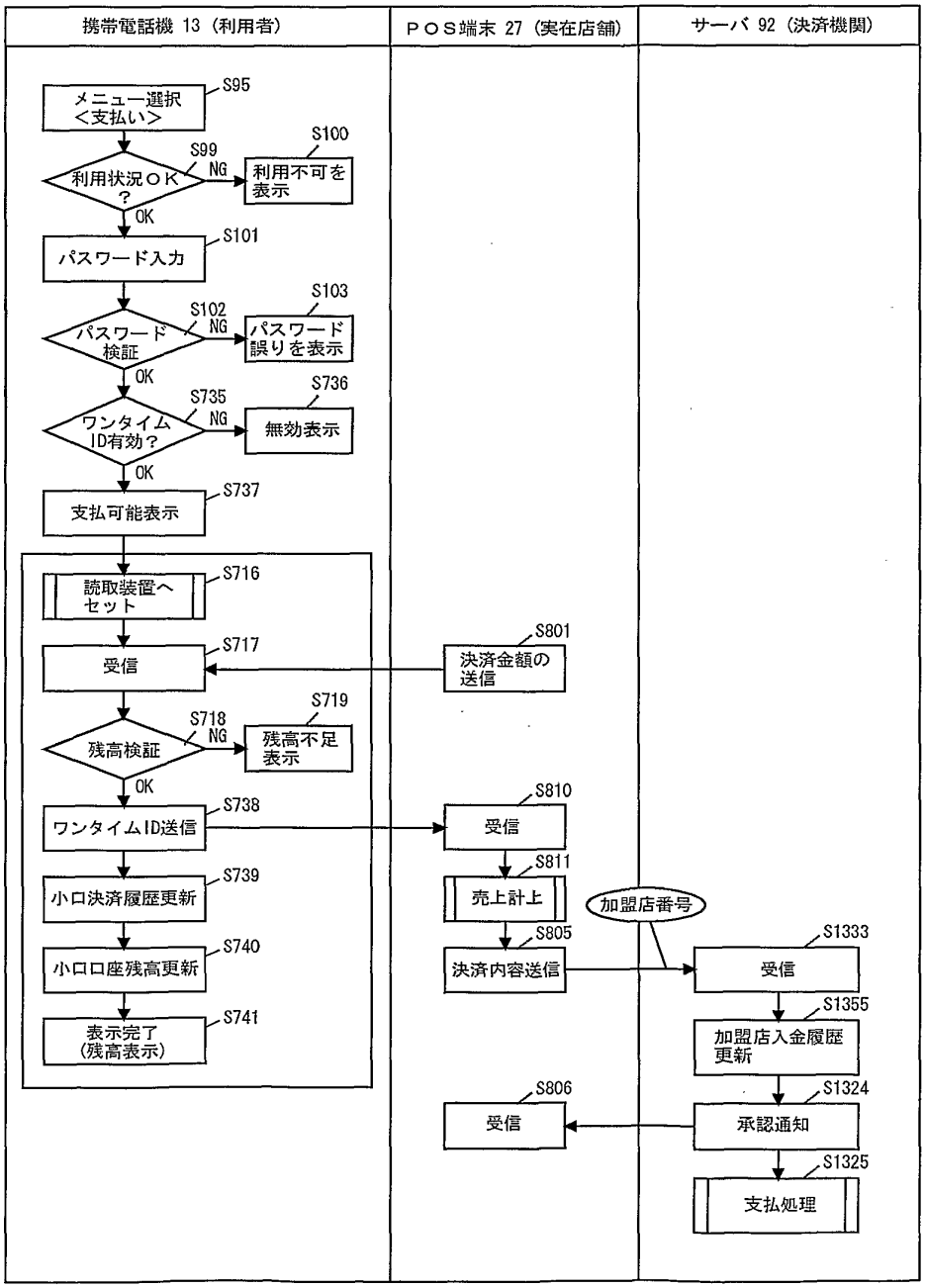

決済機関90
915
912
914
910
110
916
920
①決済内容の送信
②入金履歴の更新
利用者情報
仮想口座(10-00001) 入出金履歴
小口口座(10-00001) 入出金履歴
仮想口座(10-00001) 決済履歴
加盟店情報
加盟店(50-00030) 入金履歴
実在店舗26 (D店)
利用者12
プリペイドカード表示 (メニュー選択)
ワンタイムID 有効日検証
残高検証
ワンタイムID送信
小口口座残高・履歴更新
13
POS端末27
決済金額
売上計上
決済内容
携帯電話機

FIG. 79


携帯電話機 13（利用者）
POS端末 27（実在店舗）
サーバ 92（決済機関）
メニュー選択 <支払い>
S95
利用状況OK ?
S99
NG
利用不可を表示
S100
OK
パスワード入力
S101
パスワード検証
S102
NG
パスワード誤りを表示
S103
OK
ワンタイムID有効?
S735
NG
無効表示
S736
OK
支払可能表示
S737
読取装置へセット
S716
受信
S717
決済金額の送信
S801
残高検証
S718
NG
残高不足表示
S719
OK
ワンタイムID送信
S738
受信
S810
小口決済履歴更新
S739
売上計上
S811
加盟店番号
小口口座残高更新
S740
決済内容送信
S805
受信
S1333
表示完了（残高表示）
S741
加盟店入金履歴更新
S1355
受信
S806
承認通知
S1324
支払処理
S1325

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05039

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60, G06F19/00

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)
Int.Cl[7] G06F17/60, G06F19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96/25828 A1 (Nokia Mobile Phones, Ltd.), 22 August, 1996 (22.08.96), page 16, lines 18 to 26; page 18, lines 22 to 25 & AU 46247/96 A & AU 696876 B & CN 1174648 A & EP 809916 A1 & FI 950685 A & FI 99071 B & JP 11-501424 A & US 5887266 A	1-33
Y	WO 92/11598 A1 (Motorola, Inc.), 09 July, 1992 (09.07.92), Figs. 5(A) to 5(E) & AT 188562 E & CA 2096730 A & DE 69131897 T & EP 564469 A1 & EP 940760 A1 & ES 2141092 T & GR 3032864 T & KR 97-07003 B1 & JP 6-501329 A & JP 3010069 B2 & US 5221838 A	1-33
Y	JP 6-121075 A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 April, 1994 (28.04.94), Par. Nos. [0026] to [0027] (Family: none)	1-33

☒ Further documents are listed in the continuation of Box C. ☐ 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 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
11 September, 2001 (11.09.01)	18 September, 2001 (18.09.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05039

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2-061786 A (NEC Corporation), 01 March, 1990 (01.03.90), Fig. 1 (Family: none)	1-33
Y	EP 416916 A2 (Fujitsu Ltd.), 13 March, 1991 (13.03.91), Column 23, line 54 to Column 24, line 6 & DE 69033207 T & ES 2136057 T & JP 3-092966 A & JP 3184196 B2 & KR 9607940 A	1-33
Y	WO 99/24892 A1 (Citicorp Development Center, Inc.), 20 May, 1999 (20.05.99), page 11, lines 5 to 29; page 14, lines 18 to 24 & AU 92346/98 A & EP 917120 A2 & JP 11-232348 A & SG 78323 A	1-33
Y	WO 98/026381 A1 (Nixu OY), 18 June, 1998 (18.06.98), Figs. 6, 7; page 16, lines 1 to 6 & AU 52246/98 A & AU 729844 B & CN 1245574 A & DE 69603971 T & EP 848361 A1 & JP 2001-507487 A & NO 992776 & US 6029151 A	1-33
Y	JP 2000-113085 A (Sony Corporation), 21 April, 2000 (21.04.00), Fig. 1 (4, 5, 8) (Family: none)	1-33
A	DUKACH, Semyon, "SNPP: A Simple Network Payment Protocol", In: *Proceedings of the Eighth Annual Computer Security Applications Conference*, 30 November, 1992 (30.11.92), pages 173 to 179	1-33

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

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０１／０５０３９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60, G06F19／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60, G06F19／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 96/25828 A1 (NOKIA MOBILE PHONES LTD) 22. 8月. 1996 (22.08.96) *16 ページ, 18–26 行; 18 ページ, 22–25 行* & AU 46247/96 A　& AU 696876 B & CN 1174648 A　& EP 809916 A1 & FI 950685 A　& FI 99071 B & JP 11-501424 A　& US 5887266 A	1–33

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
11.09.01	18.09.01
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 阿波　進　５Ｌ　９１６８ 電話番号　０３－３５８１－１１０１　内線　３５６１

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 92/11598 A1 (MOTOROLA INC) 9. 7月. 1992 (09.07.92) *図5A–5E* & AT 188562 E　& CA 2096730 A & DE 69131897 T　& EP 564469 A1 & EP 940760 A1　& ES 2141092 T & GR 3032864 T　& KR 97-07003 B1 & JP 6-501329 A　& JP 3010069 B2 & US 5221838 A	1–33
Y	JP 6-121075 A（日本電信電話株式会社） 28. 4月. 1994 (28.04.94) *段落[0026]–[0027]* (ファミリーなし)	1–33
Y	JP 2-061786 A（日本電気株式会社） 1. 3月. 1990 (01.03.90) *図1* (ファミリーなし)	1–33
Y	EP 416916 A2 (FUJITSU LTD) 13. 3月. 1991 (13.03.91) *コラム23, 54行 — コラム24, 6行* & DE 69033207 T　& ES 2136057 T & JP 3-092966 A　& JP 3184196 B2 & KR 9607940 A	1–33
Y	WO 99/24892 A1 (CITICORP DEVELOPMENT CENTER INC) 20. 5月. 1999 (20.05.99) *11ページ, 5–29行; 14ページ, 18–24行* & AU 92346/98 A　& EP 917120 A2 & JP 11-232348 A　& SG 78323 A	1–33

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 98/026381 A1 (NIXU OY) 18. 6 月. 1998 (18.06.98) 図 6, 7; 16 ページ, *1–6 行* & AU 52246/98 A　& AU 729844 B & CN 1245574 A　& DE 69603971 T & EP 848361 A1　& JP 2001-507487 A & NO992776　& US 6029151 A	1–33
Y	JP 2000-113085 A (ソニー株式会社) 21. 4 月. 2000 (21.04.00) *図 1（4, 5, 8 を見よ）* (ファミリーなし)	1–33
A	DUKACH, Semyon, SNPP: A Simple Network Payment Protocol, in *Proceedings of the Eighth Annual Computer Security Applications Conference*, 30 November 1992 (30.11.92), pp 173–179.	1–33

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071354 A2

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

(21) International Application Number: PCT/CA02/00272

(22) International Filing Date: 4 March 2002 (04.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/272,300 2 March 2001 (02.03.2001) US

(71) Applicant *(for all designated States except US)*: **SOFT TRACKS ENTERPRISES LTD.** [CA/CA]; Suite 1258, 13351 Commerce Parkway, Richmond, British Columbia V6V 2X7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SWAIN, Alan, L.** [CA/CA]; 9740 Snowdon Avenue, Richmond, British Columbia V7A 2M1 (CA). **WOO, Kevin, K., M.** [CA/CA]; 10368 - 167th Street, Surrey, British Columbia V4N 1Z2 (CA).

(74) Agent: **FASKEN MARTINEAU DUMOULIN LLP**; Toronto Dominion Bank Tower, Box 20, Suite 4200, Toronto Dominion Centre, Toronto, Ontario M5K 1N6 (CA).

(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, 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:
— *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.

WO 02/071354 A2

(54) Title: SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

(57) Abstract: A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorise top-up payment of the prepaid service.

SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

BACKGROUND OF THE INVENTION

Payments in commercial transactions have evolved over time, from cash transactions, to credit card transactions to present day payment via electronic devices. Each step in the evolution has spawned its own industry and infrastructure, and successive levels in the evolution have built on the existing infrastructure. Collectively these infrastructures and processes are referred to as the payment industry.

While wireless and Internet technologies are fuelling change within the current payment industry, there is a need for new innovative payment solutions, which leverage the hard earned trust of existing financial institutions. It is the eventual goal to effect a transformation of the payment industry by enabling secure and trusted payments, in any form of tender, via any electronic device.

In general, mobile e-commerce (m-commerce) is defined as online purchasing of goods and services, including subscription based services, such as news, music and financial services, using a mobile phone service. A major challenge inhibiting widespread adoption of m-commerce solutions today is that purchasers often do not trust a mobile device as a secure way of making online payments.

A first step in overcoming this challenge is to involve the wireless carrier as the merchant in selling its own prepaid subscription service in real time. Mobile carriers currently provide three prepay top up solutions. In the first solution, customers purchase a card such as a magnetic stripe card or similar encoding mechanism to indicate that the customer has paid a predetermined prepaid value for the card. These so-called "prepaid vouchers" are purchased at retail outlets. The code on the prepaid voucher is read by the purchaser and communicated either directly on the phone with a carrier customer service representative, or through the carrier's IVR (Interactive Voice Response) system. The code represents a monetary value, which may be added

to the balance of the customer's prepaid account maintained by the carrier. A second solution is payment via credit card, wherein credit card information is either communicated to a carrier's customer service representative via voice or through a PC based web interface. A third solution involves customers prepaying for airtime through automated telemachines (ATM's). This solution is similar to prepaid vouchers in that a code printed on the ATM receipt is communicated to the carrier's customer service representative or entered through the carrier's IVR system.

As may be seen, none of the above solutions allow immediate, secure, authenticated and non-repudiable prepay top up of the customers pre paid value via the customer's wireless telephone or similar device. Because of this, current pre-paid solutions are not as successful as anticipated.

It is thus an objective of the present invention to mitigate some of the above disadvantages.

SUMMARY OF THE INVENTION

One objective of the present invention is to enable authenticated credit transactions and real time payment for top-up of prepaid cellular phones, which uses existing interfaces at both the cell phone carrier network and at the financial institution effecting the top up payment.

In accordance with this invention there is provided a method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorize top-up payment of the prepaid service

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1 is schematic diagram of a payment system according to the present invention;

Figure 2 is a schematic diagram of a payment system according to one embodiment of the invention;

Figure 3 is a schematic diagram of a payment system according to another embodiment of the invention;

Figures 4, 5, 6 and 7 show ladder diagrams for use-case scenarios of the system of figure 3.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description like numerals refer to like structures in the drawings. For convenience, the definitions, acronyms, and abbreviations used in the description are listed in table 1

Table I

Acronym/ Abbreviation	Expansion
TGS	Transaction Gateway Server
AS	Application Server
RTP	Real Time Payment
MWS	Merchant Wallet Server
VTS	Virtual Terminal Server
IVR	Interactive Voice Response
MT	Mobile Terminal
CDPD	Cellular Digital Packet Data

Acronym/ Abbreviation	Expansion
ASCII	American Standard Code for Information Interchange

Referring now to Figure 1, there is shown a block diagram of the main components in a system 100 for facilitating prepaid-type transactions according to an embodiment of the present invention. This system includes an application server (AS) 120 for processing transaction requests from at least one wireless device 122, such as a cellular telephone, the application server 120 is also capable of forwarding transactions to an acquiring financial institution 124a or an issuing financial institution depending on whether the transaction is, respectively, a credit card transaction or a real time payment (RTP) transaction. A real time payment transaction refers to a payment mechanism where funds from the purchaser's bank account are debited in near real time. The system 100 also includes a merchant wallet server (MWS) 126, which acts as a proxy between a Virtual Terminal Server (VTS) and one or more electronic wallets (e-Wallets) 130 containing user credit card numbers, bank ATM card numbers or bank account numbers, stored value account numbers, billing addresses and shipping addresses stored in a carrier subscriber database 132. The MWS is able to extract information from the e-wallets130 and present them in a form that can be used by the VTS. In effect, the MWS acts as a front end to the VTS, enabling the support of m-commerce.

Credit card and RTP transactions may also be sent through a transaction gateway server (TGS) 134 to the acquiring bank's 124a interface.

The system 100 may also include carrier's IVR server 136, which transmits payment information to the AS. Payment information captured by a carrier's IVR system is sent to the AS in the same manner as that of a WAP enabled phone. Information entered by the IVR system is combined with information stored at the carrier's subscriber database. Credit card and RTP transactions are then routed to a TGS. The

TGS is an optional intermediary in communication with the various financial institutions.

The prepaid transactions of the present invention are facilitated by payment applications (PA) running on the AS. The AS is a multi-application server, which allows for a variety of different payment methods and tender types. The payment applications have support for tender types such as credit card, cash, cheque, and e-Wallets. The e-Wallets themselves may contain references to credit cards, bank accounts, and stored value accounts. In addition, the payment application has an Enterprise Reporting feature allowing reports on usage per subscriber. An important feature of the AS is the ability to route the prepay transactions to the appropriate processing interface based on the payment type. In the case of WAP enabled digital phones, the owner of the prepaid mobile device communicates with the AS via the payment application residing on the AS. Information entered by the user, along with information kept within the carrier's prepaid database / e-Wallet is aggregated in the AS. The AS handles payment types as described below.

The payment types supported by the system 100 are generally credit card transactions and RTP transactions. With each of these payment types, there are different levels of device 122 and user authentication, different interface requirements, and differences in response mechanisms. The transaction types implemented will require mutual resolution and agreement between the parties.

Non-Face-To-Face Transactions Using Credit Cards

In a credit card transaction, only the credit card number of the prepaid user is stored in a subscriber e-Wallet 130. This is what is currently used to effect Internet based payment. There is no authentication for the card or account, no authentication of the owner of the card or account and no authentication of the owner's intent to complete the transaction as is evidenced in a card present credit card transaction when the card is swiped and the owner signs the receipt or as is evidenced in an on-line debit transaction when the card is swiped and the owner of a debit card enters a secret PIN

associated with the debit card. Rather, this type of transaction is typically called a Mail Order Telephone Order (MOTO) transaction. This does not fulfill general requirements of a go-to-market strategy for m-Commerce as these types of transactions can be easily repudiated and hence are highly subject to fraud. This invention enables m-commerce transactions that can generally not be repudiated. This invention meets the general requirements for non-repudiation of ensuring that the transaction process itself requires something that only the consumer has in possession and that the consumer intended to complete the transaction by requiring consumer to securely disclose to the system, something that only the consumer knows. The challenge of m-Commerce to achieve this is made even more difficult as often, the consumer and the merchant are not face-to-face as is the case with a an on-line credit card or an on-line debit card transaction.

Credit Card with Subscriber Device Authentication

Subscriber handset identities (SID) are commonly used within cellular networks to authenticate user phones. In this case, a credit card number is associated with the phone's secure identity to satisfy the concept of a virtual card. Currently, to effect a card present transaction, the card must be physically swiped and the data (called track2 data) on the magstripe of the card must be captured. If a trust relationship is set up between the carrier and the financial institution, the combination of the phone's secure identity and credit card number represents an equivalent risk to a card present transaction. This may be referred to as a "virtual card present transaction".

Credit Card with Subscriber Device & Password Authentication

Building on the virtual credit card transaction, a password can be associated with the subscriber's e-Wallet. The password is used to authenticate the owner of the e-Wallet (i.e. the subscriber), allowing access to the associated virtual credit card contained in the e-Wallet. User authentication lowers the risk of fraud involved in using a virtual credit card. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation.

RTP through EFT

The AS can route RTP transactions via the TGS to an Electronic Funds Transfer (EFT) interface of banks. This mechanism transfers money from the subscriber's bank account to the merchant's bank account overnight. The attractiveness of EFT is the ability to handle transactions for all banks through one interface. The EFT backend deals with the transfer of funds between the individual banks. A limitation of the EFT interface is that payment transfers are typically delayed up to 24 hours, and are not immediate. Responses are typically batched into one file and extracted from the EFT interface, when the file is available. Therefore, prepay top up transactions may take up to 24 hours before receiving a response from the bank, hence failing to meet a real time acknowledgement requirement.

This delay is addressed in one of several ways. A first option is that the financial institution processes and acknowledges an EFT transaction in real time in a scenario where the merchant (i.e. carrier) account and subscriber account is within its own domain. A second option is that a notification is sent to the subscriber some time in advance when the number of minutes still remaining in the subscriber's prepay account is below a certain level so that the 24-hour delay is inconsequential.

RTP through Real Time Payment Gateway

The AS can route RTP transactions via the TGS to evolving bank interfaces. The goal of these interfaces is to process funds transfer transactions in real time. Transactions belonging to the bank, hosting the interface, may be processed in real time. These interfaces, often based on XML standards such as OFX, provide a real time confirmation for a given transaction, unlike an EFT interface. Real time responses allow a subscriber to issue a payment transaction online and wait for the acknowledgement. Within this scenario the financial institution can only process and acknowledge transactions in real time when the subscriber holds an account at that bank.

Debit Transactions

With Debit transactions networks such as the Interac^{tm} network the underlying principles of authentication can be satisfied with today's cellular security and

authentication technologies, hence making debit transactions acceptable, most especially in the closed environment of prepay.

As described earlier, the MWS acts as a proxy between the VTS and e-Wallets that hold subscriber credentials. The MWS combines information from e-Wallets and information entered from either the carrier's IVR system or the WAP based prepay application. The information is used to construct a credit or RTP transaction. Once a successful response message is received, the MWS is responsible for notifying both the user of the mobile device, and the carrier's prepay subscriber database. The response can be sent to the WAP based prepay application or the carrier's IVR system. In the case that the subscriber database held at the carrier receives a successful response, the appropriate amount is added to the user's prepaid account.

Another feature of the MWS is the ability for a merchant to be authenticated as part of the transaction. Merchant credentials can be securely stored within the MWS and can be included in the transaction details, if the bank requires. This is a major step towards having the ability to authenticate both the subscriber and the merchant in a financial transaction. Optionally, if a PKI-enabled MWS is used, merchant credentials can be encrypted and digitally signed before sending the authentication to the bank. There are three e-Wallet configurations that the MWS supports.

Bank Hosted Wallet Server 140

The bank may choose to hold all of the subscriber's credentials within their own e-Wallet. The carrier's subscriber database is used as an authentication mechanism to enable payment through the bank e-Wallet. One authentication scheme involves the use of a token, which is stored at the subscriber database held at the carrier, and that token is used to extract subscriber credentials within the bank e-Wallet. This token can take the form of a PKI public key or certificate. If the prepay user has multiple e-Wallets with different banks, the carrier's subscriber database facilitates an authentication mechanism for each of the e-Wallets.

Carrier Hosted Wallet Server 130

The MWS can operate in an environment where a carrier hosts an e-Wallet. User information, along with credit card numbers and bank account numbers is held within the carrier's e-Wallet. This information is sent to the MWS, when a prepay top up transaction is being constructed. There is also a method for the MWS to update the user prepay account information at the carrier's subscriber database. In this scenario, the carrier subscriber database is proxied by the e-Wallet server. Therefore, once a response from a top up transaction is received, the MWS passes the details of the response to the e-Wallet server. The e-Wallet server, in turn, updates the users prepay account information held within the subscriber database.

Carrier and Bank Jointly Hosts the Wallet Server

The bank may choose to hold some of the e-Wallet credentials such as bank account information. They may also choose to hold only those credentials pertaining to the particular bank. This is an example of a multiple e-Wallet implementation. The MWS is capable of supporting connections to multiple e-Wallet servers whether they are hosted at the carrier or the bank.

While the overall system components, and payment types handle by the system have been describe above, the security mechanism implemented by the system 100 is now described.

Device Authentication

A device can be authenticated before any interactions with a financial institution. Carriers use subscriber identity authentication mechanisms and other security measures to safeguard the security and identity of a cellular phone. This technology, especially in the digital space has proven effective in authentication of mobile phones. The MWS solution builds on the carrier's authentication mechanisms. A devices authenticated identity is associated with a credit card number creating the notion of a virtual credit card. In actuality, the carrier's authentication procedure will enable the first step in granting access to a subscriber's e-Wallet that contains a subscriber's virtual credit cards. A password is used to authenticate the owner of the e-Wallet and

forms the second step in granting access to transact with the virtual credit cards in the e-Wallet.

User Authentication

To enable a prepay transaction, the carrier may choose to authenticate the user before accepting the transaction. There may be one or more passwords depending on the payment method. Typically, an e-Wallet password will be required to initiate a top up transaction. A second password may be needed to affect an RTP transaction. This is similar to an online bill payment scenario, where typically a username and password is required. The subscriber handset identity (SID) is used in place of the username. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation. PKI technologies will be implemented as these technologies mature within cellular devices.

Communication between Infrastructure Components

Standard Secure Sockets Layer (SSL) communications protocols are implemented on wide-area communications.

Referring to figure 2, there is shown another embodiment of the system 200 of the present invention. The system 200 comprises four interfaces into the AS, namely a carrier IVR system, carrier WAP gateway, carrier subscriber database via the e-Wallet, and the financial institution's acquiring interface via the TGS. It is noted that the carrier subscriber database is represented as an entity that accepts transaction responses and exception codes.

This implementation builds on the existing carrier infrastructure and requires only changes to the carrier's IVR system interface so that the IVR system communicates with the AS. All other four interfaces stay intact.

Prepay top up transactions can originate from either the carrier's IVR system or a WAP enabled phone. The IVR system communicates via an IP based connection into the AS business logic. XML based communications protocols may be used.

Whereas, the WAP enabled phone will access a prepay application hosted at the AS. Although, both mechanisms use different input strategies, the backend processing does not change.

The e-Wallet function has been split up into two components. The first component is an implementation of a simple e-Wallet for storage of subscriber payment information. The second component is the subscriber database that is currently in use at the carriers. When a top up transaction is created, user credentials are retrieved from the e-Wallet. This information is combined with the information entered by the user to affect the transaction. Once a transaction response has been received, an account update request is sent from the MWS to the subscriber database via the e-Wallet server. Both types of payment types are supported: credit card, and RTP.

Referring to figure 3, there is shown a further embodiment of an implementation of the system 100. In this scenario, the subscriber prepay database function has been separated from the client e-Wallet server. Once a transaction response has been received, an account update request is sent from the MWS directly to the subscriber database. Transaction details may be sent to the e-Wallet server to provide the subscriber with a transaction history.

Referring to figure 4, there is shown a ladder diagram describing a first use case for the embodiment of figure 3. This use-case describes a subscriber initiated prepay via WAP Phone scenario.

This scenario is a two-step transaction. The subscriber is involved in two phone sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The prepay application may be accessible from either the WAP browser's default menu or by typing the URL of the application. The second session involves pushing an alert back to the subscriber. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The subscriber ID of the

mobile device held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 4 may be described as follows:

1. The subscriber enters the URL of WAP prepay application.
2. The carrier network validations ESN and MIN of subscriber phone.
3. Secure session is initiated with WAP gateway and prepay application host – the subscriber ID (SID) of the phone is passed to the application in the request header.
4. The subscriber is prompted by the prepay application for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
5. Prepay application builds an XML based message and sends the message to the MWS. The request will minimally contain the SID for device authentication and optionally a password for subscriber authentication.
6. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
7. Based on the SID, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.
8. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
9. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay

transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

10. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

11. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction.

12. The prepay web server sends a second XML based request to the MWS, which is an authorization request (confirmation) of the original prepay transaction.

13. The MWS sends the payment request to the VTS using an XML based protocol.

14. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

15. The TGS processes the transaction through the financial payment gateway.

16. The TGS receives a transaction response from the financial payment gateway.

17. The transaction response is routed back from the TGS to the VTS.

18. The transaction result is passed from the VTS to the MWS.

19. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

20. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

21. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

22. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 5, there is shown a ladder diagram describing a second use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via WAP Phone scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, described with reference to figure 4, we are certain that the push alert will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, a push alert is generated from the system. The subscriber acts on this push alert to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 5 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is

generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.

2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.

4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

6. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction. The subscriber is also prompted for

additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.

9. The MWS sends the payment request to the VTS using an XML based protocol.

10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

11. The TGS processes the transaction through the financial payment gateway.

12. The TGS receives a transaction response from the financial payment gateway.

13. The transaction response is routed back from the TGS to the VTS.

14. The transaction result is passed from the VTS to the MWS.

15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

18. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 6, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a Subscriber Initiated Prepay Via IVR System scenario.

This scenario is a two-step transaction. The subscriber is involved in two IVR sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The second session involves pushing an alert back to the subscriber. The push alert takes the form of a phone call to the subscriber device. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The phone number (Mobile Identity Number, MIN) held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 6 may be described as follows:

1. The subscriber dials the IVR system through the subscriber's device. The prepay application is selected from the list of options.
2. The carriers network validations ESN and MIN of subscriber phone.
3. The subscriber is prompted by the IVR system for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
4. The IVR system builds the appropriate XML based message and sends the message to the MWS. The request will minimally contain the MIN for device authentication and optionally a DTMF password for subscriber authentication. The assumption is that caller ID is activated for the subscriber's device; therefore, the IVR system receives and passes through the MIN of the phone.

5. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

6. Based on the MIN, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.

7. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

8. An XML based response message is sent back to the IVR system. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback in the next.

9. An IVR callback to the subscriber phone is performed using the MIN sent from the MWS. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

10. The subscriber authorizes the prepay transaction through the IVR system.

11. The IVR system sends a second XML based request to the MWS, which is an authorization (confirmation) request of the original prepay transaction.

12. The MWS sends the payment request to the VTS using an XML based protocol.

13. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

14. The TGS processes the transaction through the financial payment gateway.

15. The TGS receives a transaction response from the financial payment gateway.

16. The transaction response is routed back from the TGS to the VTS.

17. The transaction result is passed from the VTS to the MWS.

18. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

19. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

20. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

21. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 7, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via IVR System scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, we are certain that the IVR callback mechanism will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, an IVR phone call is generated from the system. The subscriber confirms through the IVR system to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 7 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.
2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.
4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback mechanism in the next step.

6. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction through the IVR system. The subscriber is also prompted for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.

9. The MWS sends the payment request to the VTS using an XML based protocol.

10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

11. The TGS processes the transaction through the financial payment gateway.

12. The TGS receives a transaction response from the financial payment gateway.

13. The transaction response is routed back from the TGS to the VTS.

14. The transaction result is passed from the VTS to the MWS.

15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may

optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

18. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Accordingly it may be seen that the system of the present invention provides a secure real-time top-up service that can be implemented in existing payment infrastructures.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, said method comprising the steps of:

(a) receiving at an application server first information indicative of the transaction device authentication;

(b) receiving at said application server second information for verification of said user; and

(c) using both said first and second information to authorize top-up payment of said prepaid service from said financial institution.

2. A method as defined in claim 1, said prepaid service being a prepaid cellular phone.

3. A method as defined in claim 2, said first information being a hardware identification of said cellular telephone.

4. A method as defined in claim 2, said second information being a personal identification number (PIN) of said user.

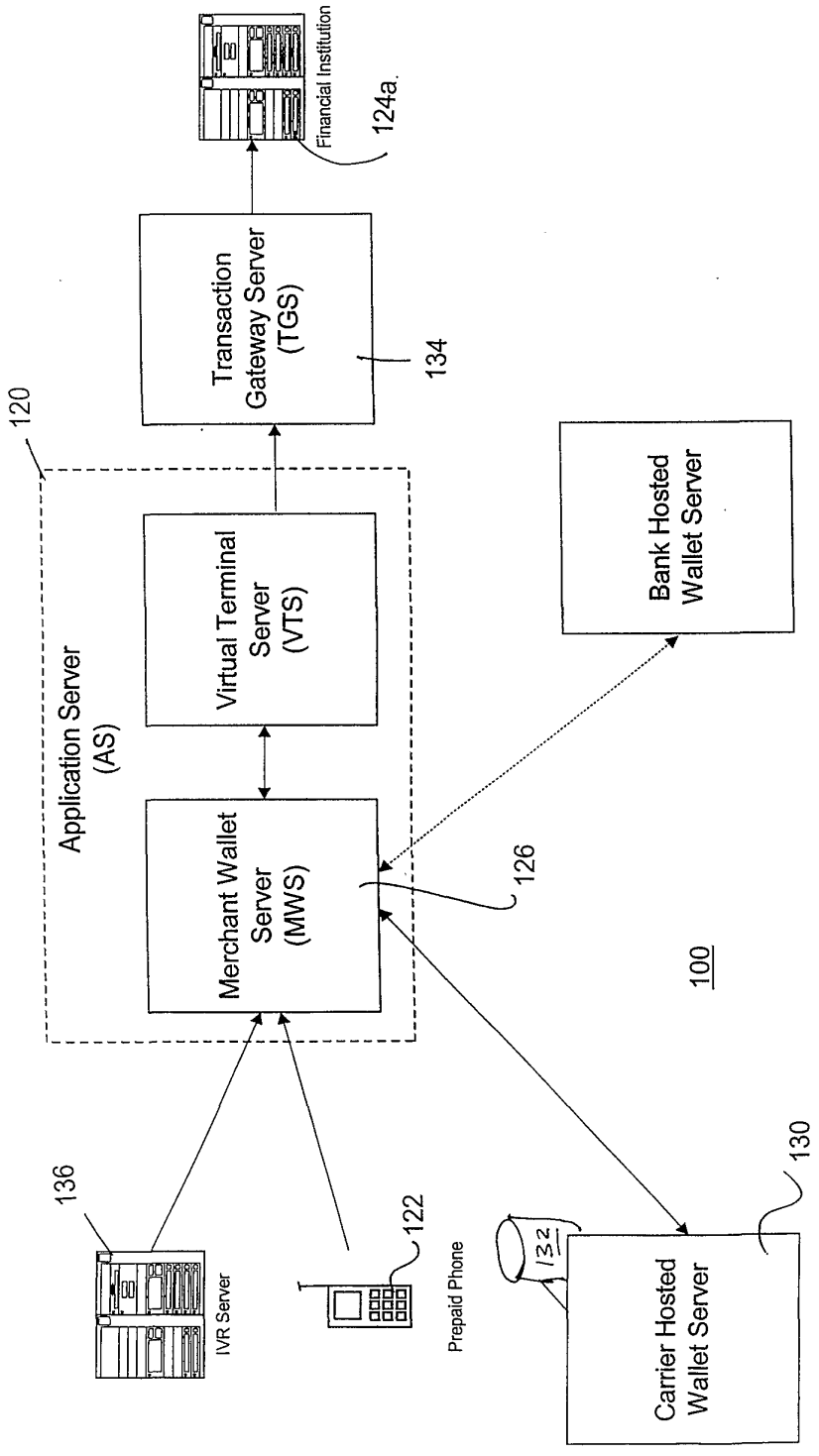

Financial Institution
124a
Transaction Gateway Server (TGS)
134
120
Application Server (AS)
Virtual Terminal Server (VTS)
Merchant Wallet Server (MWS)
126
Bank Hosted Wallet Server
100
136
IVR Server
122
Prepaid Phone
132
130
Carrier Hosted Wallet Server

Figure 1

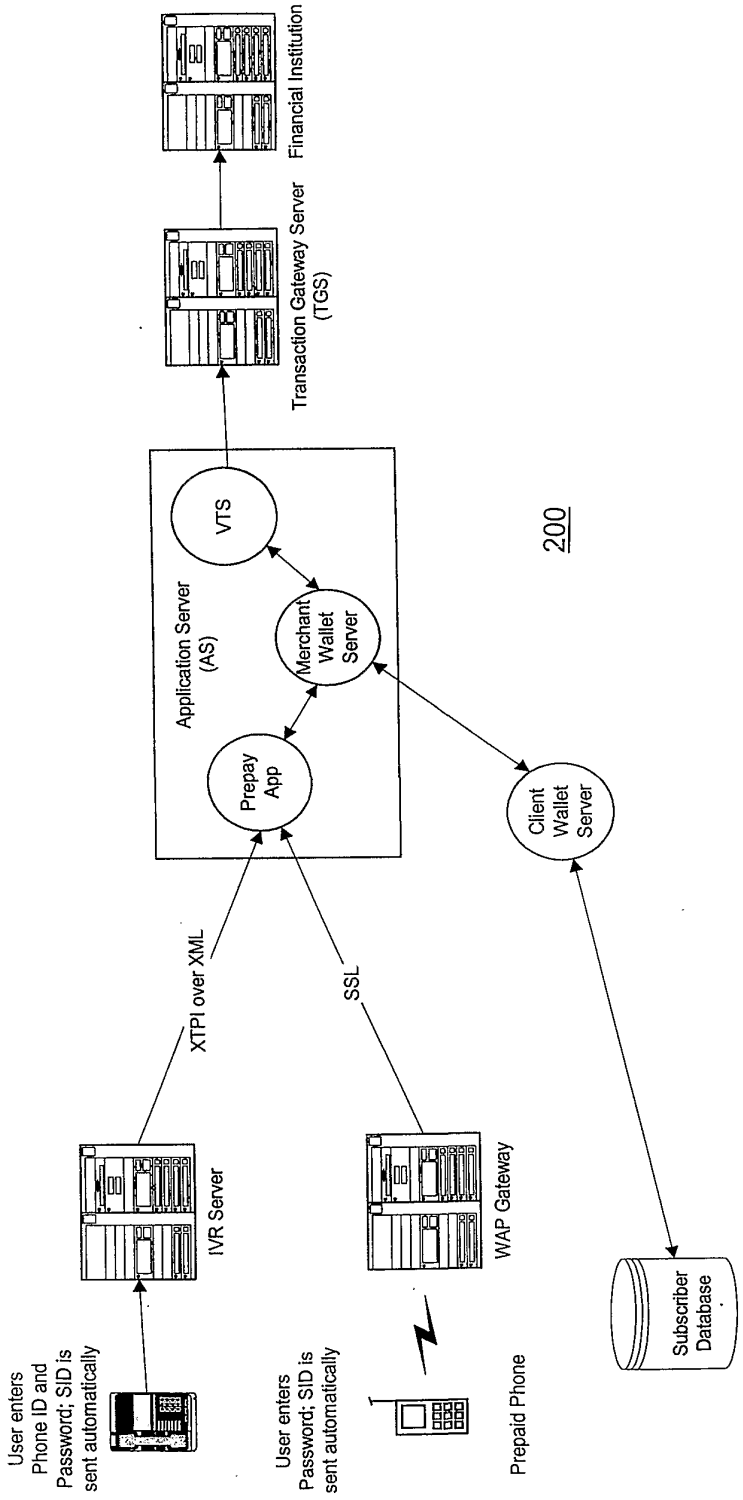

Financial Institution
Transaction Gateway Server (TGS)
VTS
Application Server (AS)
Merchant Wallet Server
Prepay App
200
Client Wallet Server
XTPI over XML
SSL
IVR Server
WAP Gateway
Subscriber Database
User enters Phone ID and Password; SID is sent automatically
User enters Password; SID is sent automatically
Prepaid Phone

Figure 2

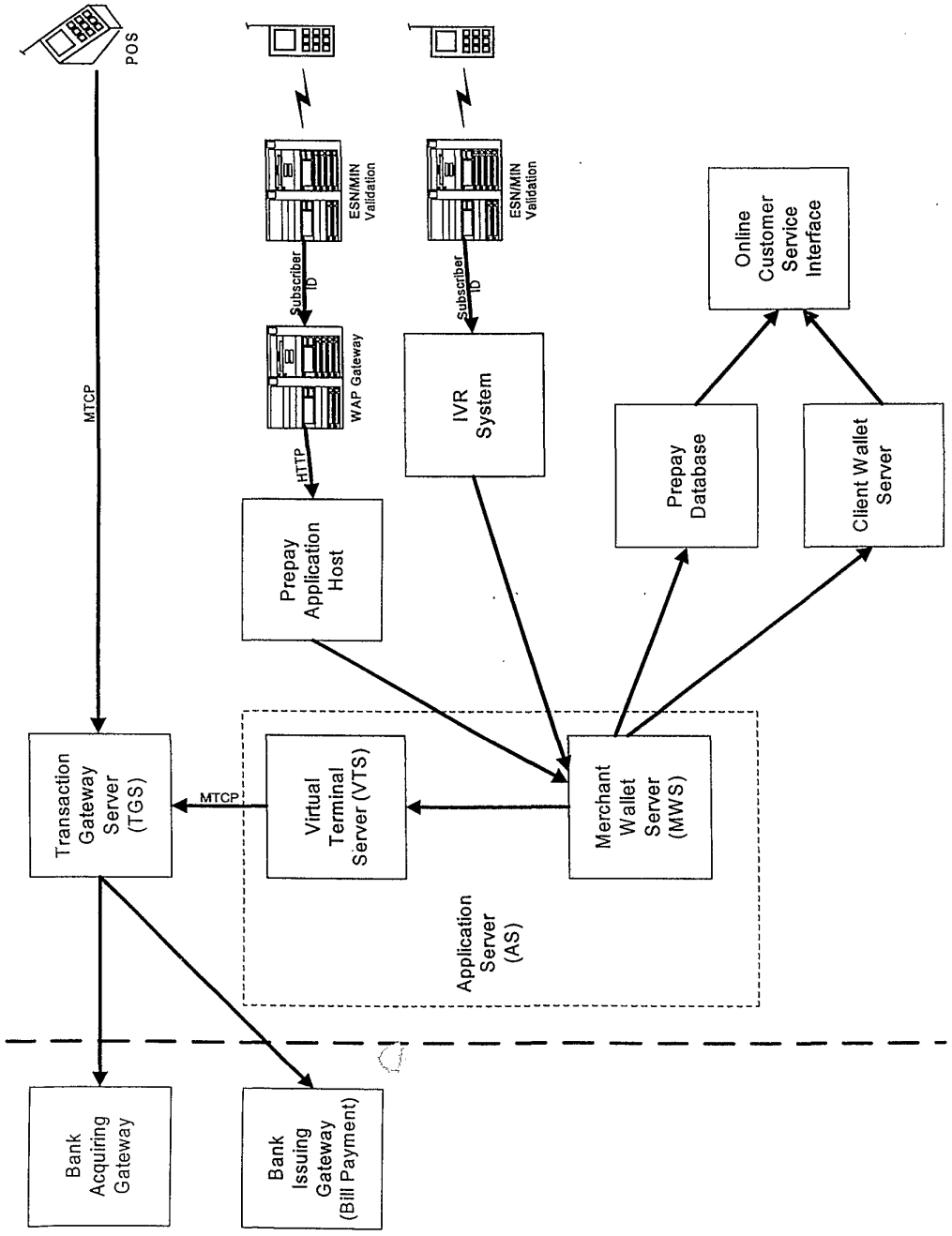

POS
MTCP
ESN/MIN Validation
ESN/MIN Validation
Subscriber ID
Subscriber ID
WAP Gateway
HTTP
IVR System
Online Customer Service Interface
Prepay Database
Client Wallet Server
Prepay Application Host
Transaction Gateway Server (TGS)
MTCP
Virtual Terminal Server (VTS)
Merchant Wallet Server (MWS)
Application Server (AS)
Bank Acquiring Gateway
Bank Issuing Gateway (Bill Payment)

Figure 3

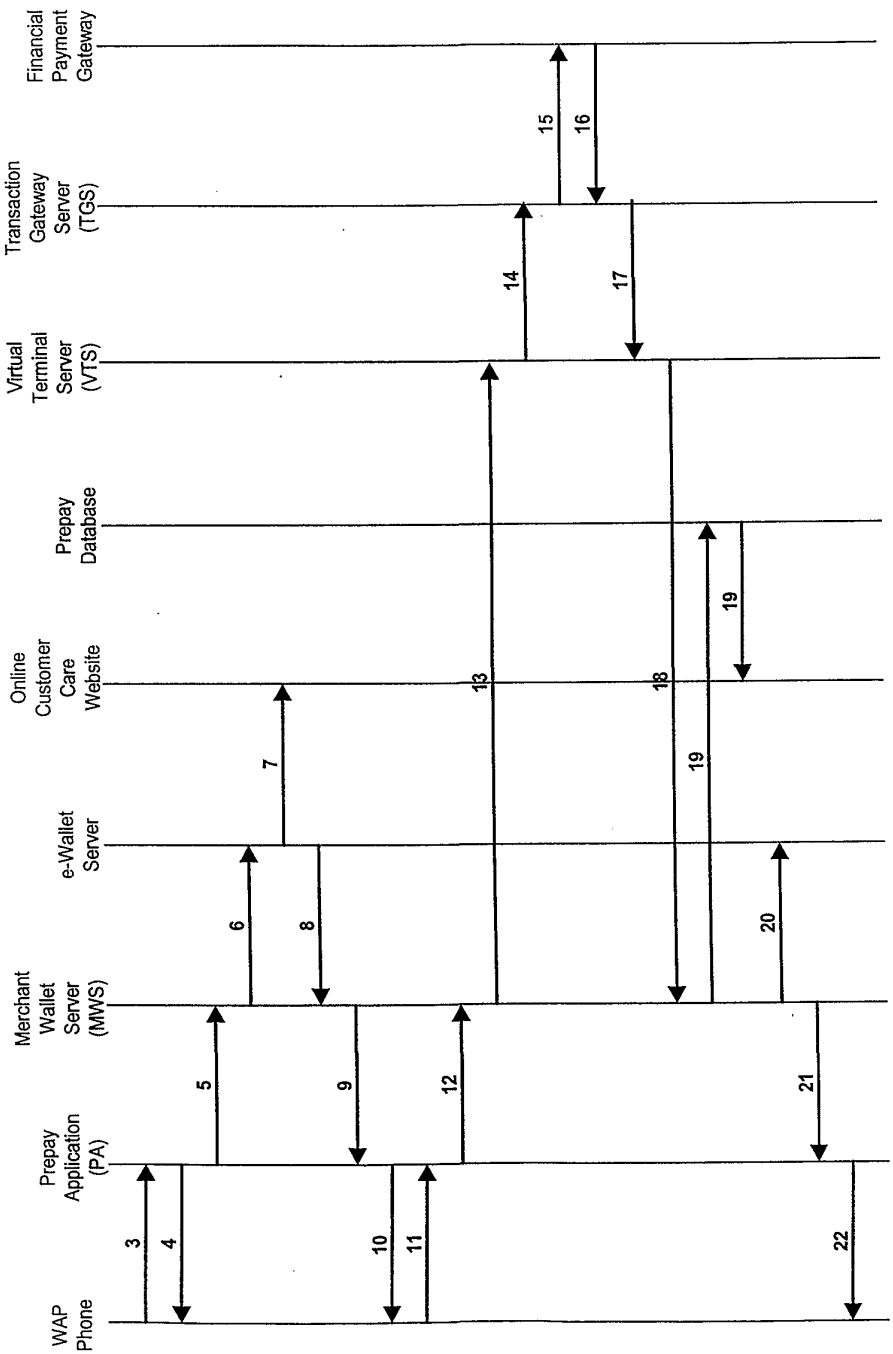

Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
Prepay Application (PA)
WAP Phone
15
16
14
17
19
13
18
19
7
6
8
20
5
9
12
21
3
4
10
11
22

Figure 4

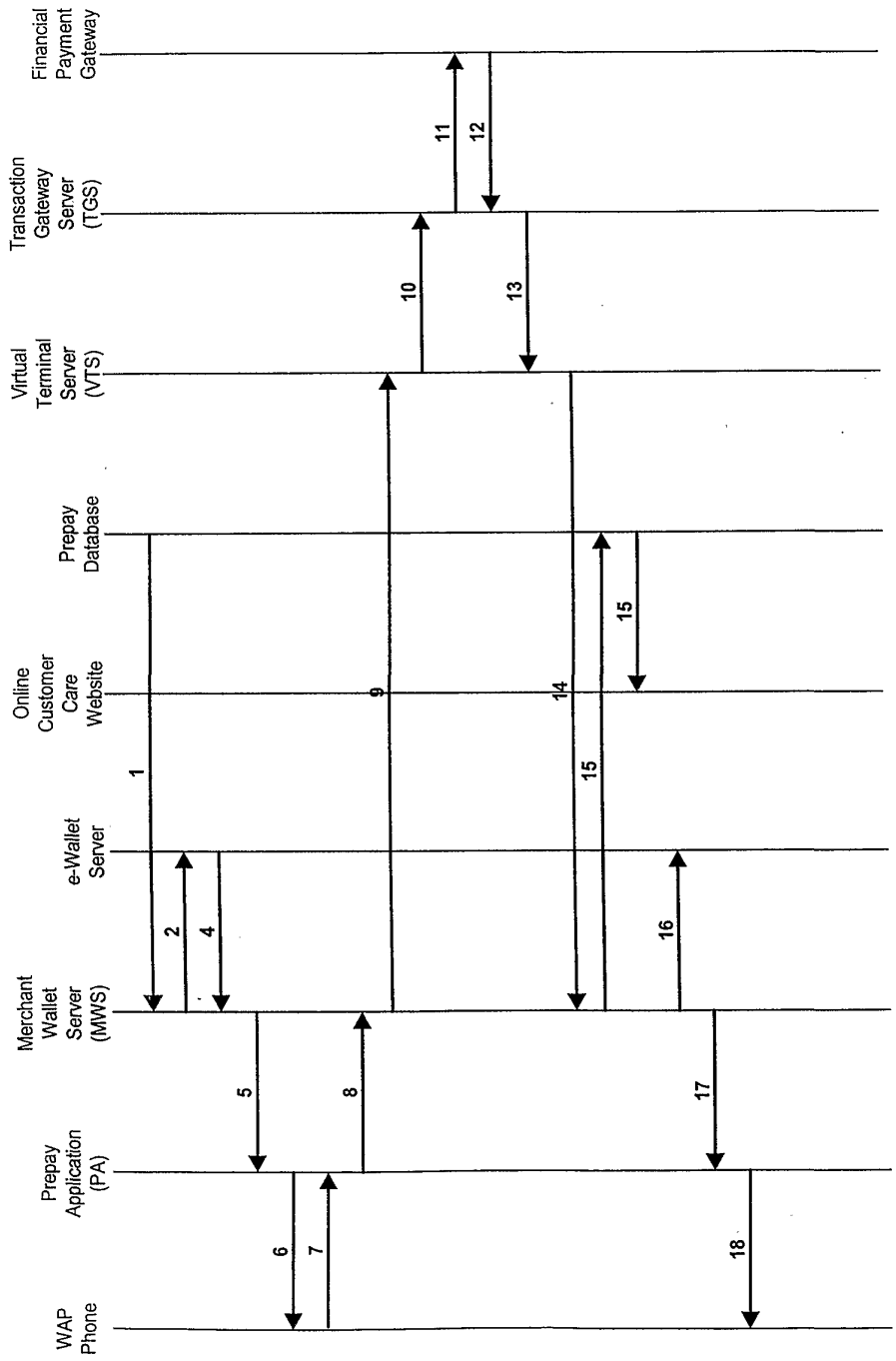

Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
Prepay Application (PA)
WAP Phone
1
2
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

Figure 5

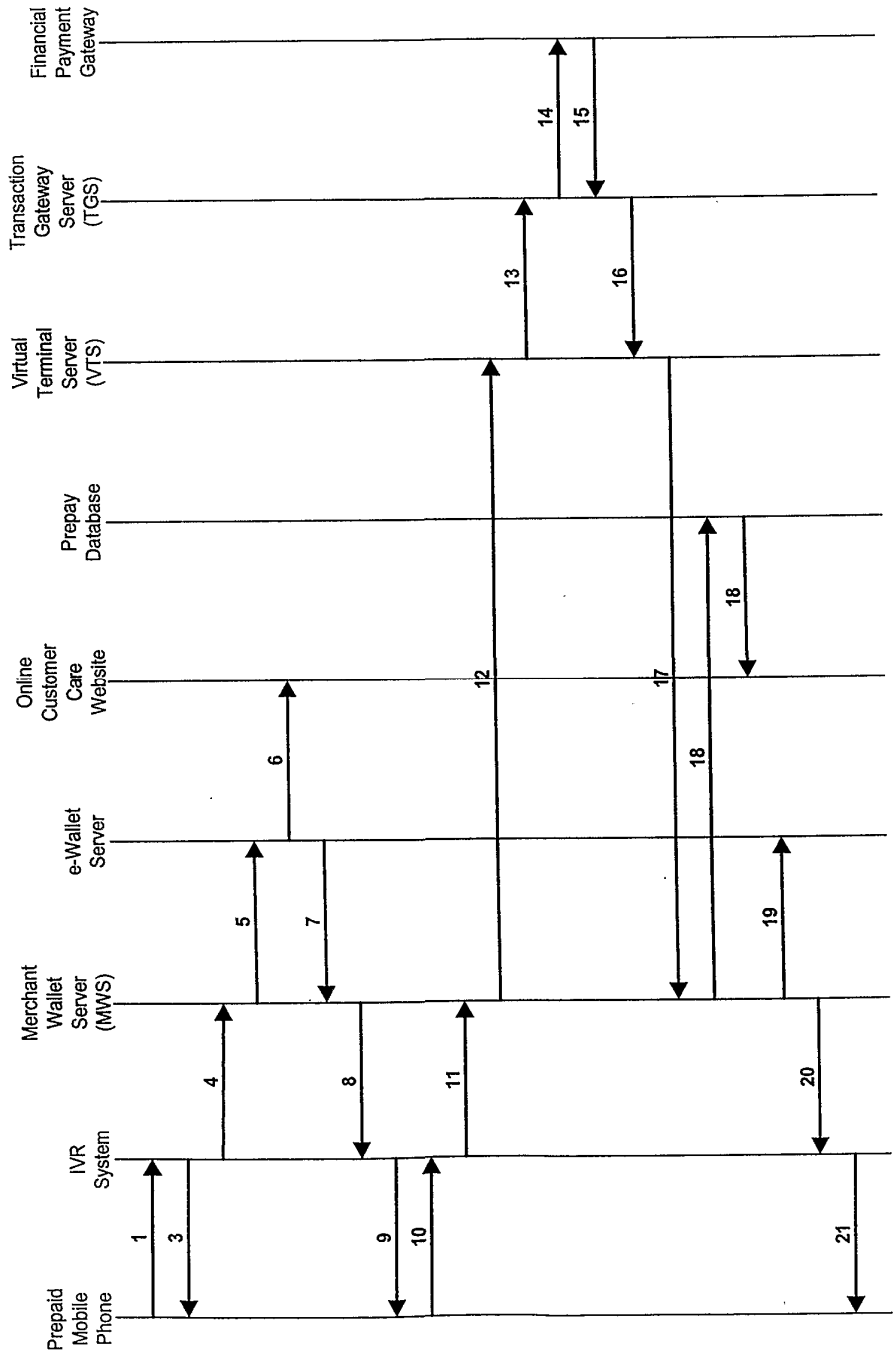

Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
IVR System
Prepaid Mobile Phone
1
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Figure 6

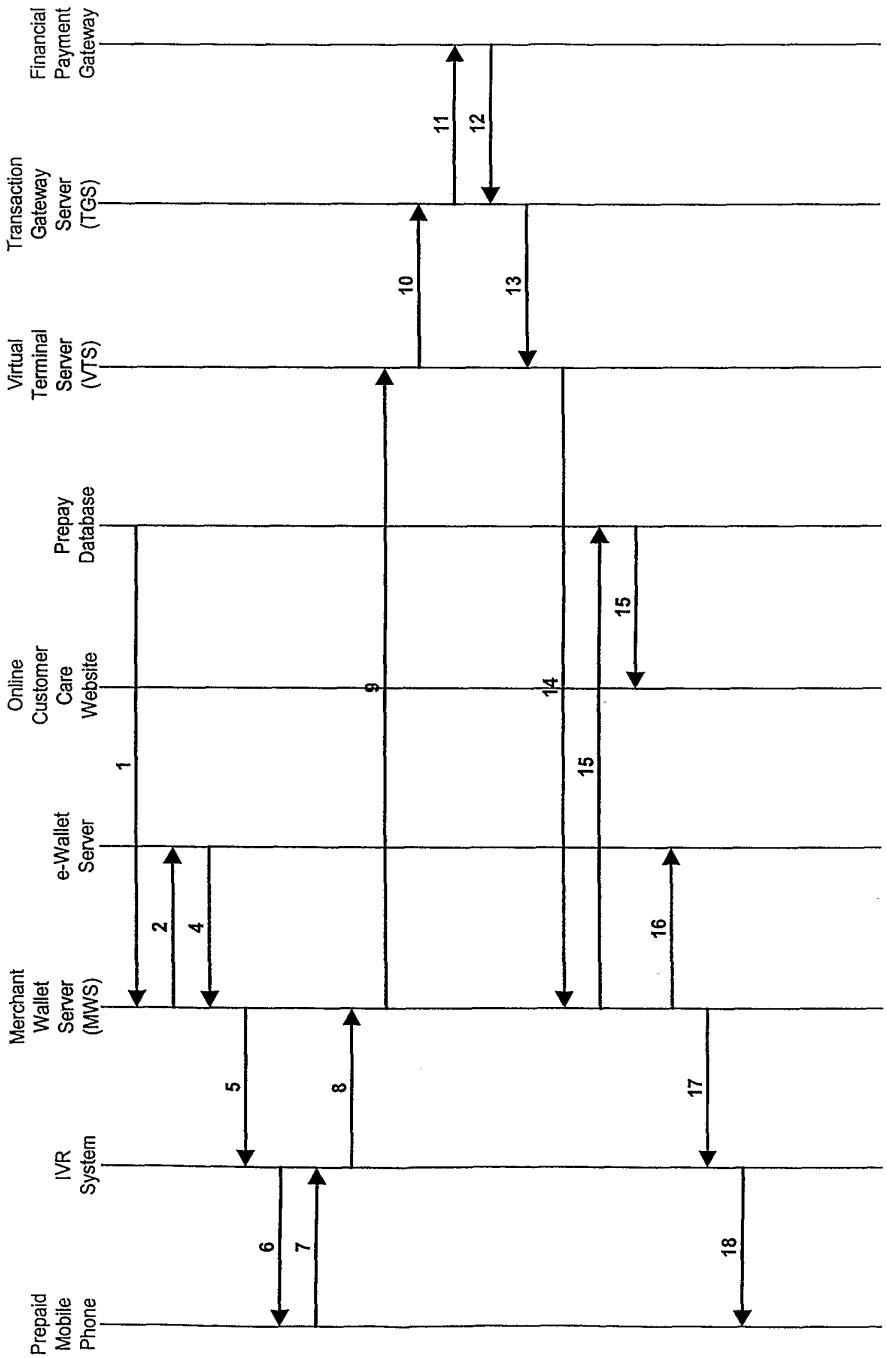

Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
IVR System
Prepaid Mobile Phone
1
2
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

Figure 7

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
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).

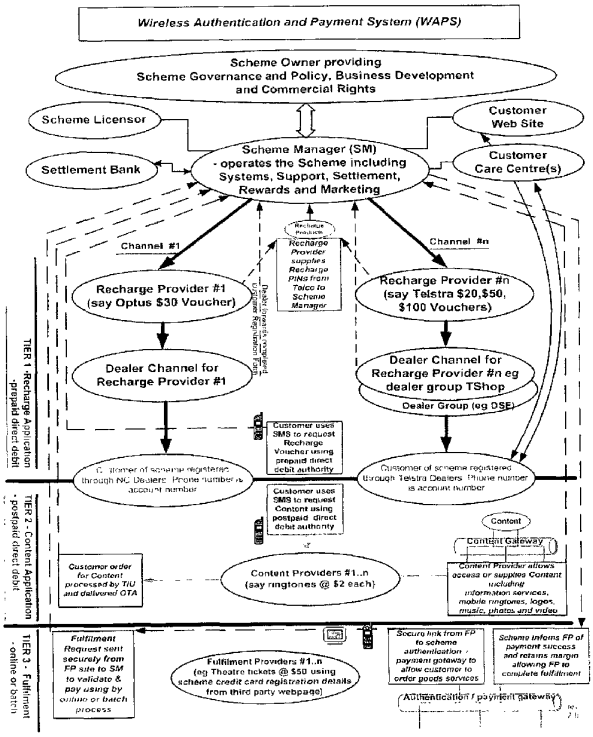
(72) Inventors; and

(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.

APPL-1002
APPLE INC. / Page 846 of 1892

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,

APPL-1002
APPLE INC. / Page 847 of 1892

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.

APPL-1002
APPLE INC. / Page 848 of 1892

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;

APPL-1002
APPLE INC. / Page 849 of 1892

- 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

APPL-1002
APPLE INC. / Page 851 of 1892

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

APPL-1002
APPLE INC. / Page 852 of 1892

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

APPL-1002
APPLE INC. / Page 853 of 1892

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

APPL-1002
APPLE INC. / Page 854 of 1892

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.

APPL-1002
APPLE INC. / Page 856 of 1892

(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

APPL-1002
APPLE INC. / Page 857 of 1892

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.

APPL-1002
APPLE INC. / Page 858 of 1892

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.

APPL-1002
APPLE INC. / Page 859 of 1892

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

APPL-1002
APPLE INC. / Page 860 of 1892

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

APPL-1002
APPLE INC. / Page 861 of 1892

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;

APPL-1002
APPLE INC. / Page 862 of 1892

- *'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;

APPL-1002
APPLE INC. / Page 863 of 1892

- 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

APPL-1002
APPLE INC. / Page 867 of 1892

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

APPL-1002
APPLE INC. / Page 868 of 1892

- 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.

APPL-1002
APPLE INC. / Page 869 of 1892

- 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

APPL-1002
APPLE INC. / Page 870 of 1892

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.

APPL-1002
APPLE INC. / Page 871 of 1892

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.

APPL-1002
APPLE INC. / Page 872 of 1892

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;

APPL-1002
APPLE INC. / Page 874 of 1892

- 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

APPL-1002
APPLE INC. / Page 877 of 1892

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

APPL-1002
APPLE INC. / Page 879 of 1892

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:-

APPL-1002
APPLE INC. / Page 881 of 1892

- 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.

APPL-1002
APPLE INC. / Page 882 of 1892

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

APPL-1002
APPLE INC. / Page 883 of 1892

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

APPL-1002
APPLE INC. / Page 889 of 1892

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

APPL-1002
APPLE INC. / Page 891 of 1892

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.

APPL-1002
APPLE INC. / Page 892 of 1892

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.

APPL-1002
APPLE INC. / Page 894 of 1892

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

APPL-1002
APPLE INC. / Page 895 of 1892

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

APPL-1002
APPLE INC. / Page 896 of 1892

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

APPL-1002
APPLE INC. / Page 899 of 1892

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

APPL-1002
APPLE INC. / Page 901 of 1892

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.

APPL-1002
APPLE INC. / Page 903 of 1892

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				
Instore/Web Registration											P web	P store	P store			
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.

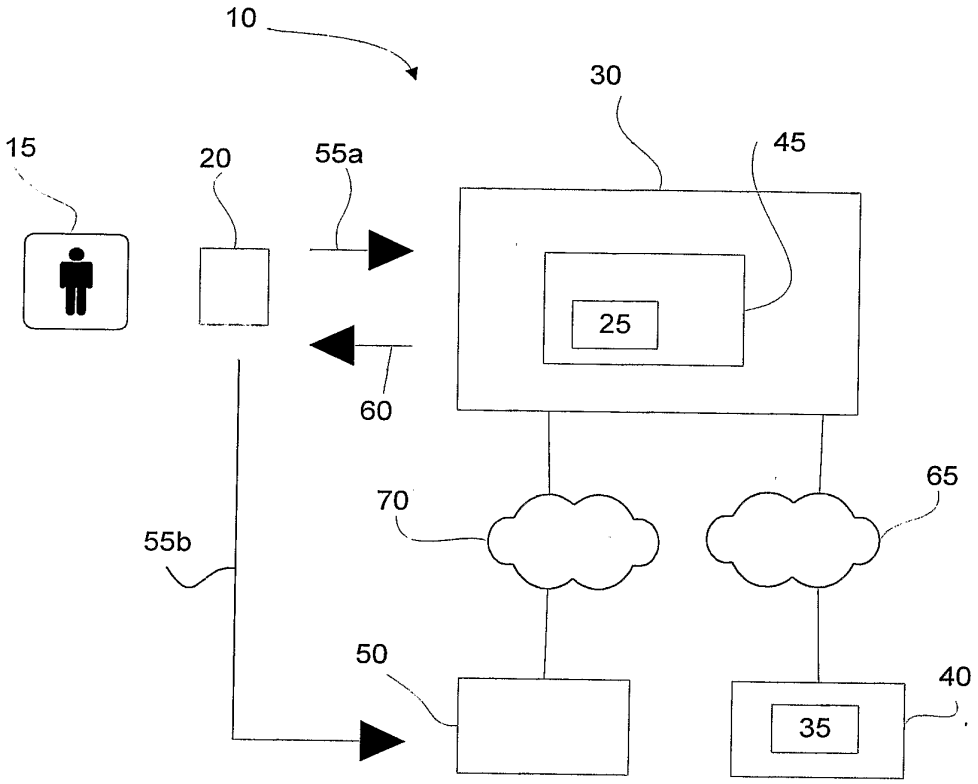
14. A system and method as claimed in claim 13; whereby the scheme allows the customer to purchase or pay for products and/or services at time of request "online" from the scheme authorised third party, if said customer has authorised the scheme to participate in such third party schemes.

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.

APPL-1002
APPLE INC. / Page 906 of 1892

Figure 1



APPL-1002
APPLE INC. / Page 907 of 1892

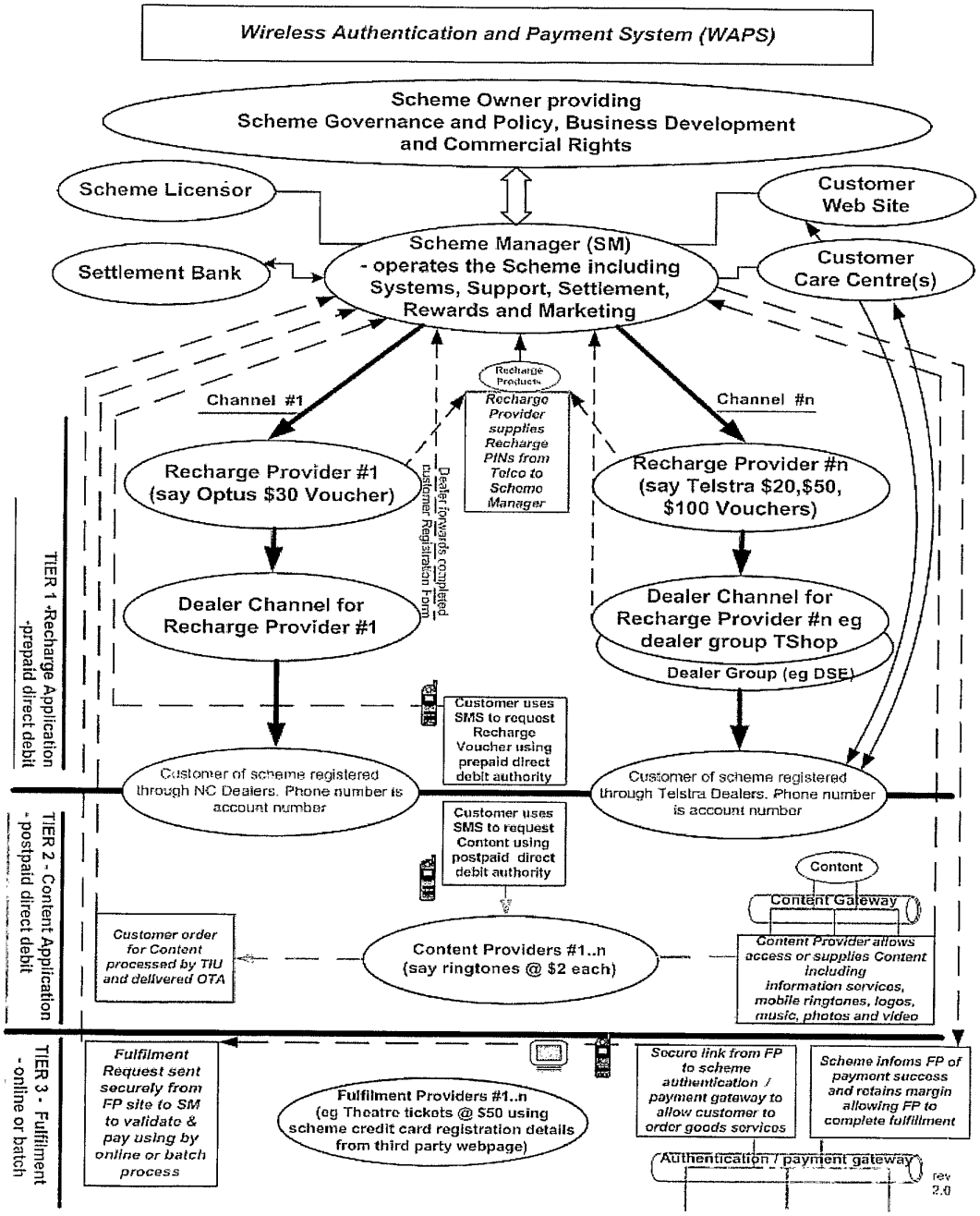


Figure 2

APPL-1002
APPLE INC. / Page 908 of 1892

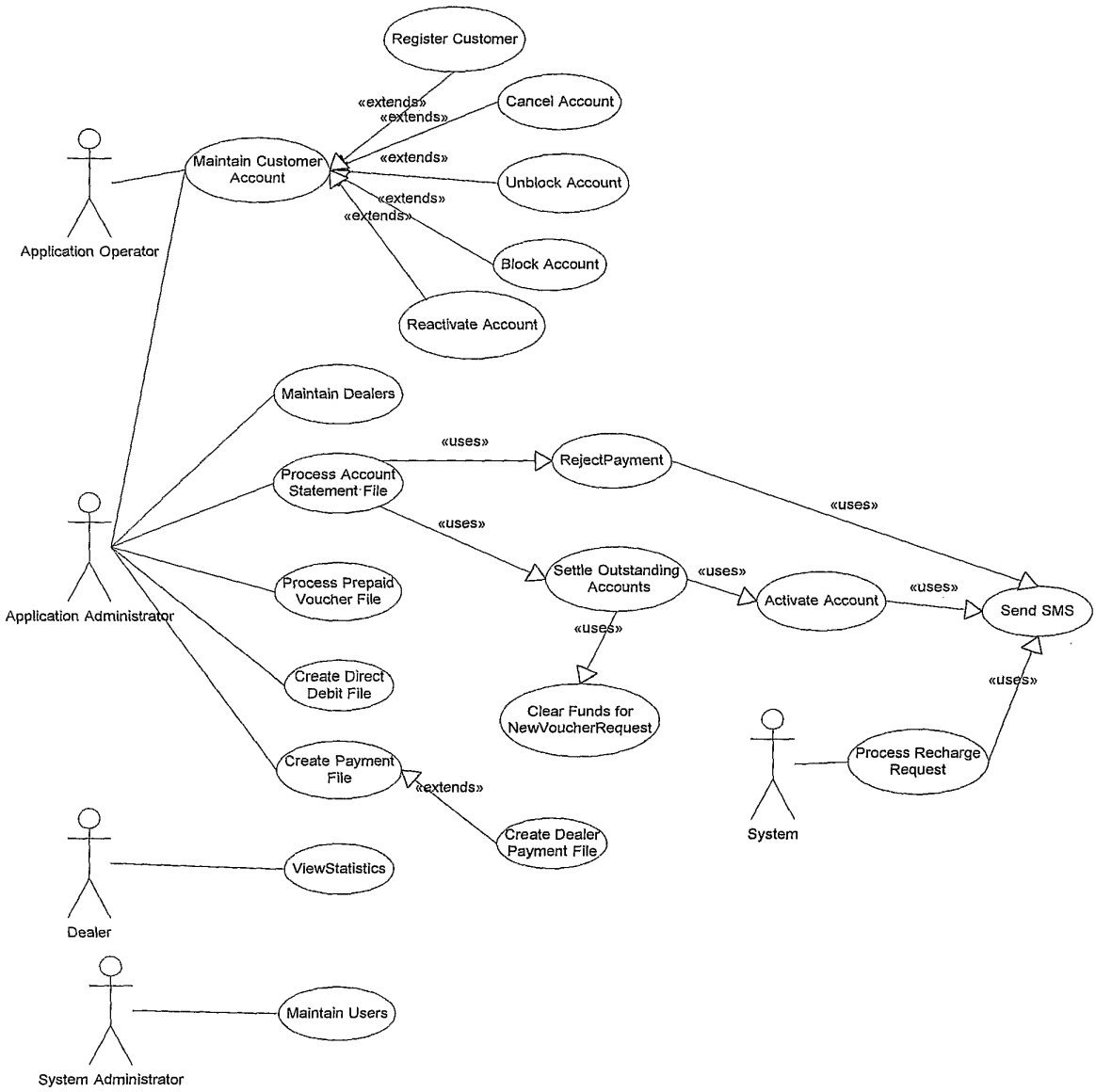


Figure 3

APPL-1002
APPLE INC. / Page 909 of 1892

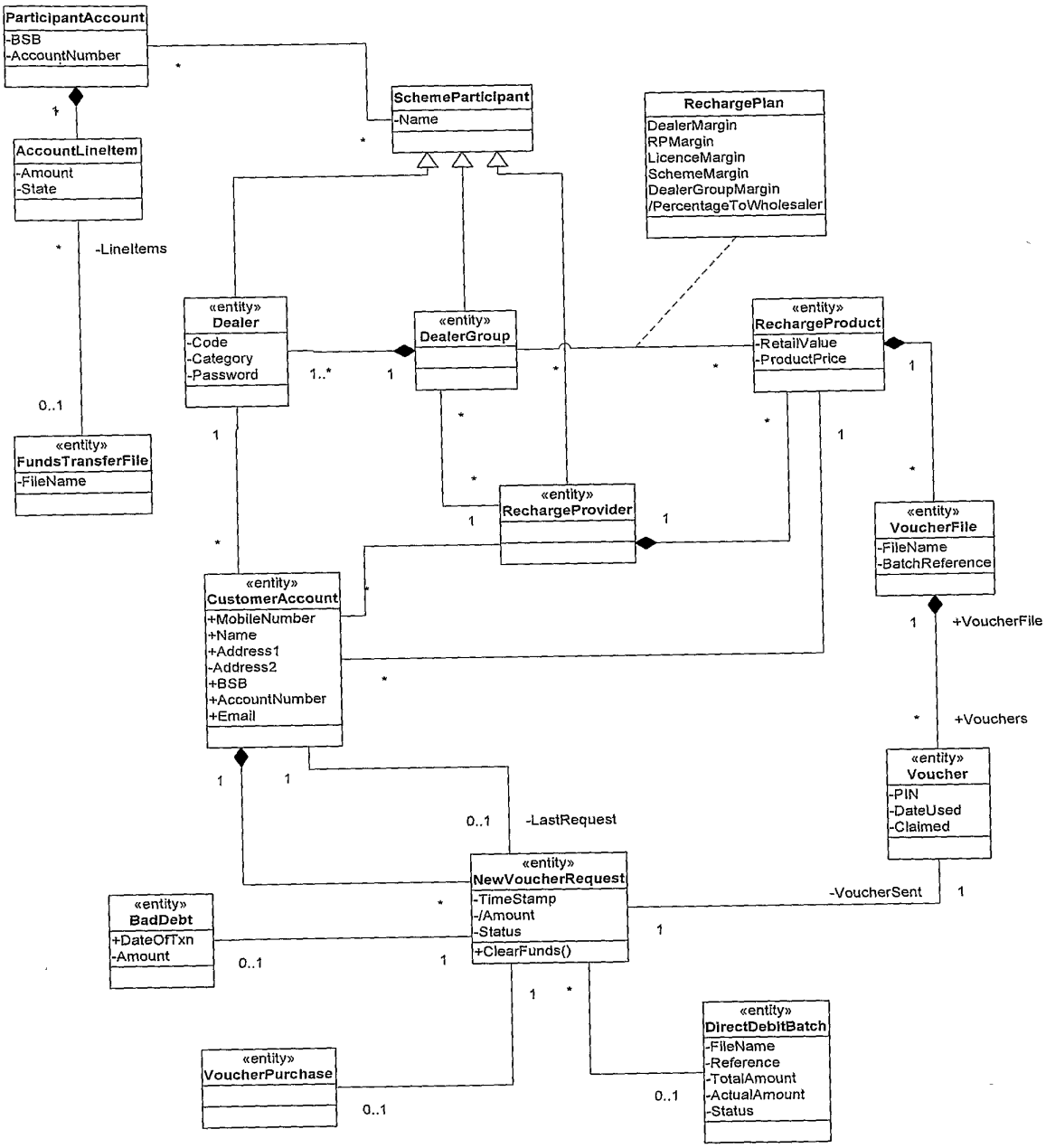

ParticipantAccount
-BSB
-AccountNumber
AccountLineItem
-Amount
-State
-LineItems
FundsTransferFile
-FileName
SchemeParticipant
-Name
RechargePlan
DealerMargin
RPMargin
LicenceMargin
SchemeMargin
DealerGroupMargin
/PercentageToWholesaler
«entity»
Dealer
-Code
-Category
-Password
«entity»
DealerGroup
«entity»
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»
DirectDebitBatch
-FileName
-Reference
-TotalAmount
-ActualAmount
-Status
«entity»
VoucherPurchase

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).

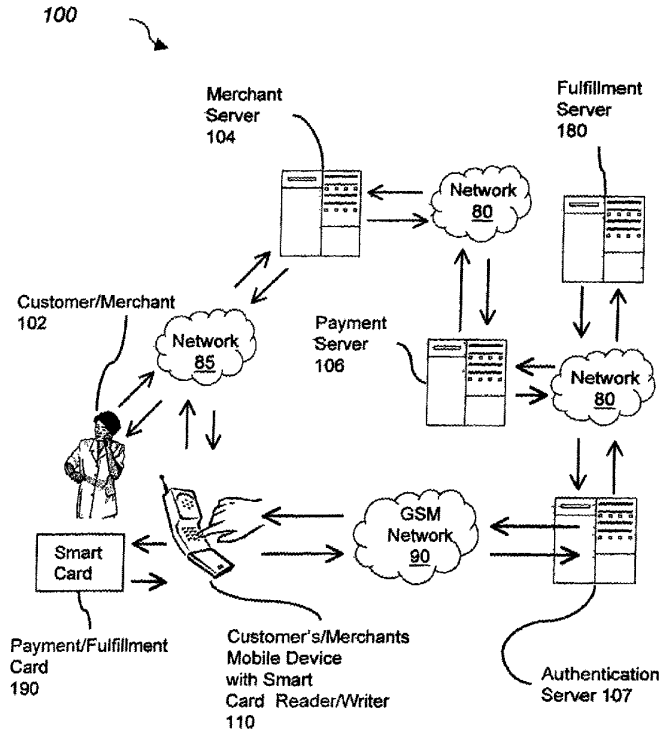
(74) Agent: **COLLINS, Aliki, K., PH., D.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(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.

APPL-1002
APPLE INC. / Page 921 of 1892

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:

APPL-1002
APPLE INC. / Page 930 of 1892

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.

APPL-1002
APPLE INC. / Page 933 of 1892

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.

APPL-1002
APPLE INC. / Page 936 of 1892

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.

APPL-1002
APPLE INC. / Page 938 of 1892

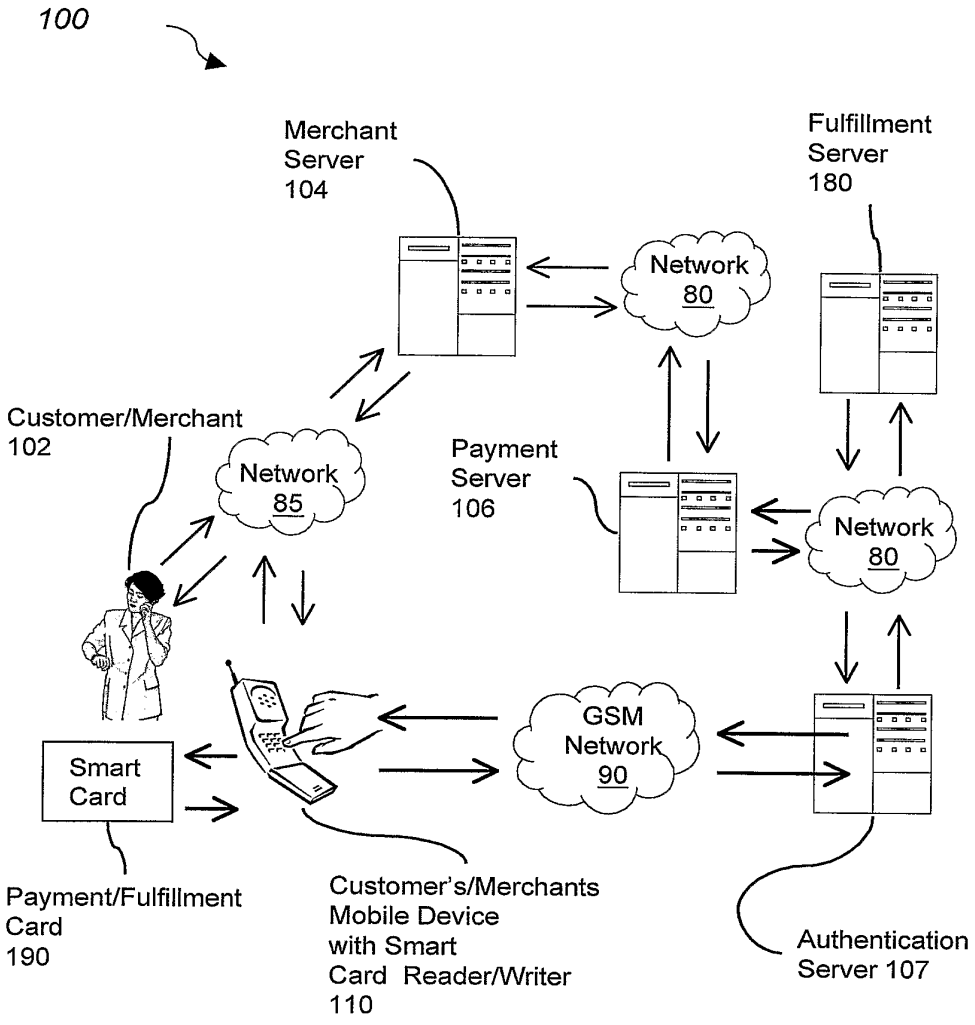

100
Merchant Server 104
Fulfillment Server 180
Network 80
Customer/Merchant 102
Network 85
Payment Server 106
Network 80
Smart Card
GSM Network 90
Payment/Fulfillment Card 190
Customer's/Merchants Mobile Device with Smart Card Reader/Writer 110
Authentication Server 107

FIG. 1

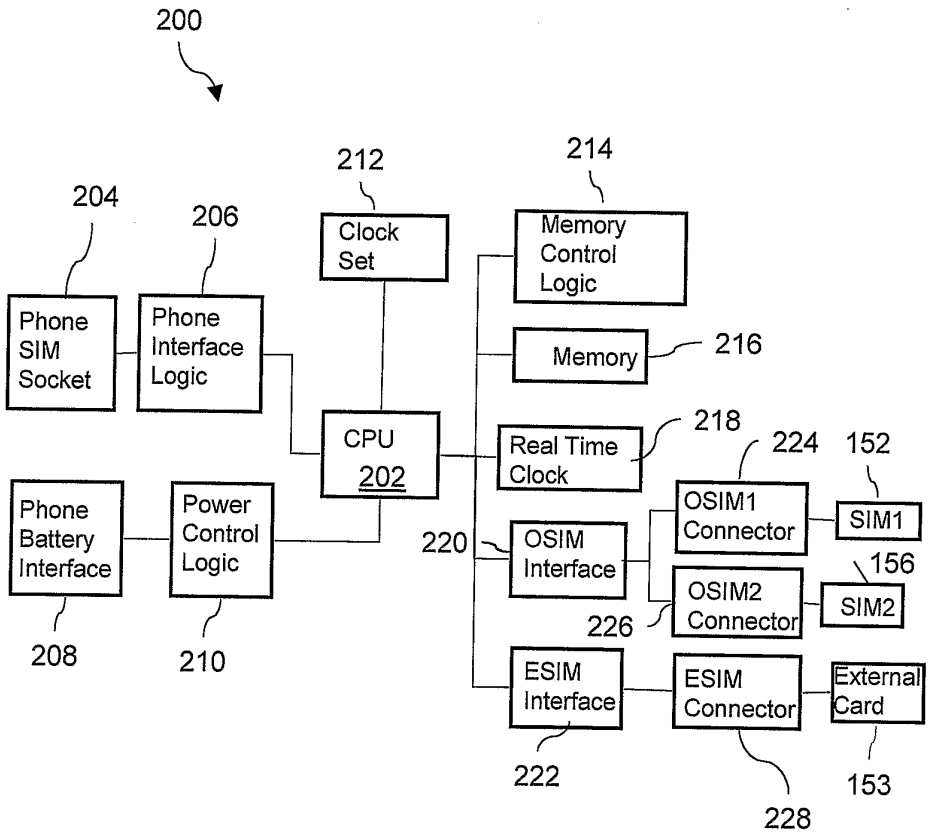


FIG. 2
(Prior Art)

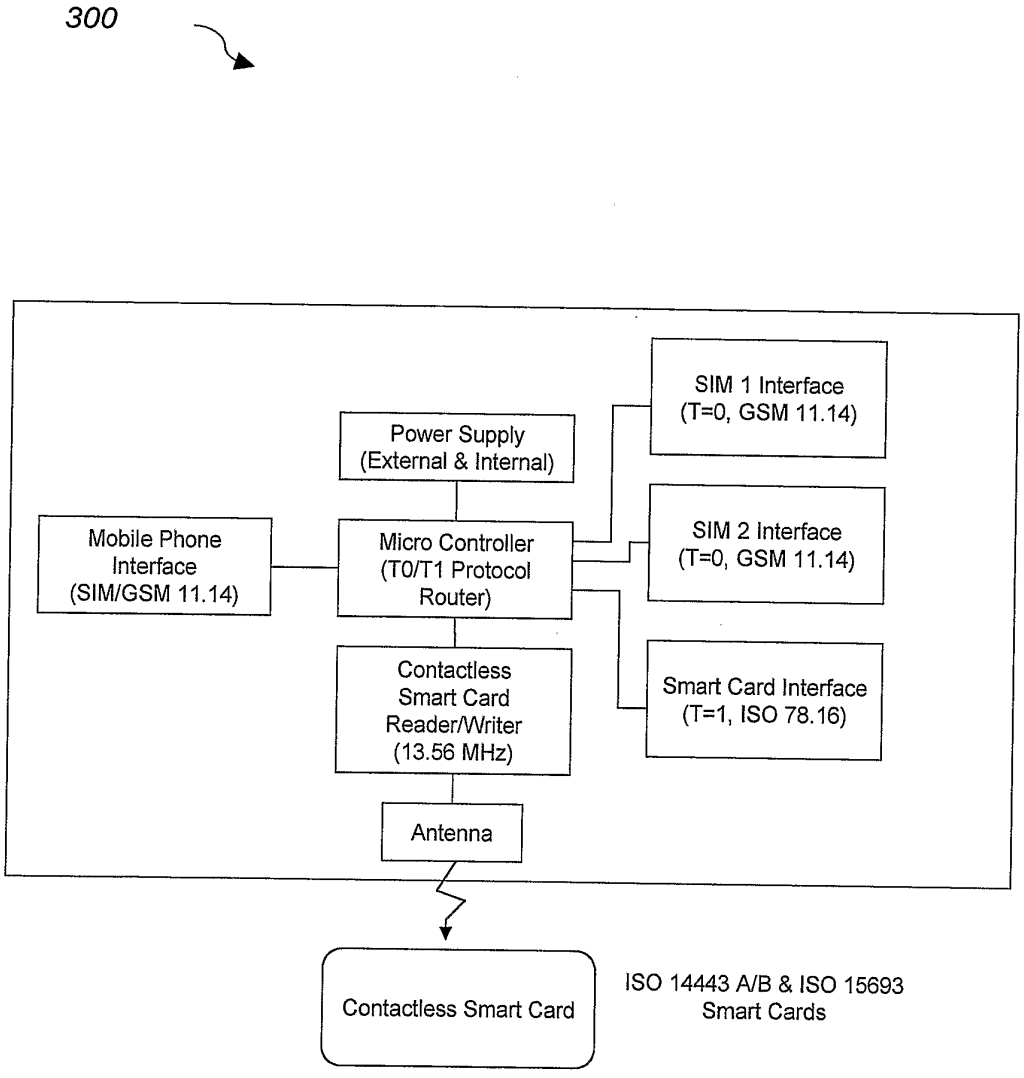

300
SIM 1 Interface
(T=0, GSM 11.14)
Power Supply
(External & Internal)
Mobile Phone
Interface
(SIM/GSM 11.14)
Micro Controller
(T0/T1 Protocol
Router)
SIM 2 Interface
(T=0, GSM 11.14)
Contactless
Smart Card
Reader/Writer
(13.56 MHz)
Smart Card Interface
(T=1, ISO 78.16)
Antenna
Contactless Smart Card
ISO 14443 A/B & ISO 15693
Smart Cards

FIG. 3

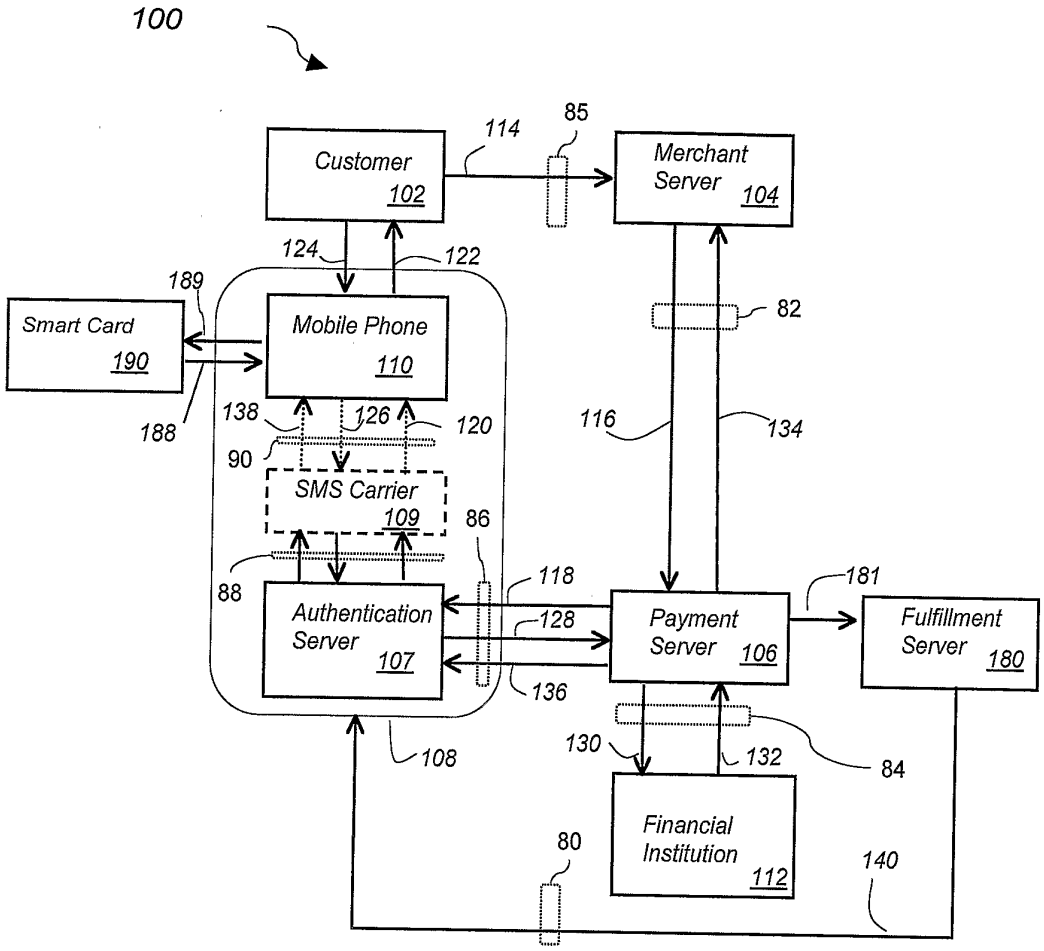

100
Customer
102
Merchant
Server
104
Smart Card
190
Mobile Phone
110
SMS Carrier
109
Authentication
Server
107
Payment
Server
106
Fulfillment
Server
180
Financial
Institution
112
114
85
124
122
189
82
138
126
120
116
134
188
90
86
118
181
88
128
136
108
130
132
84
80
140

FIG. 4

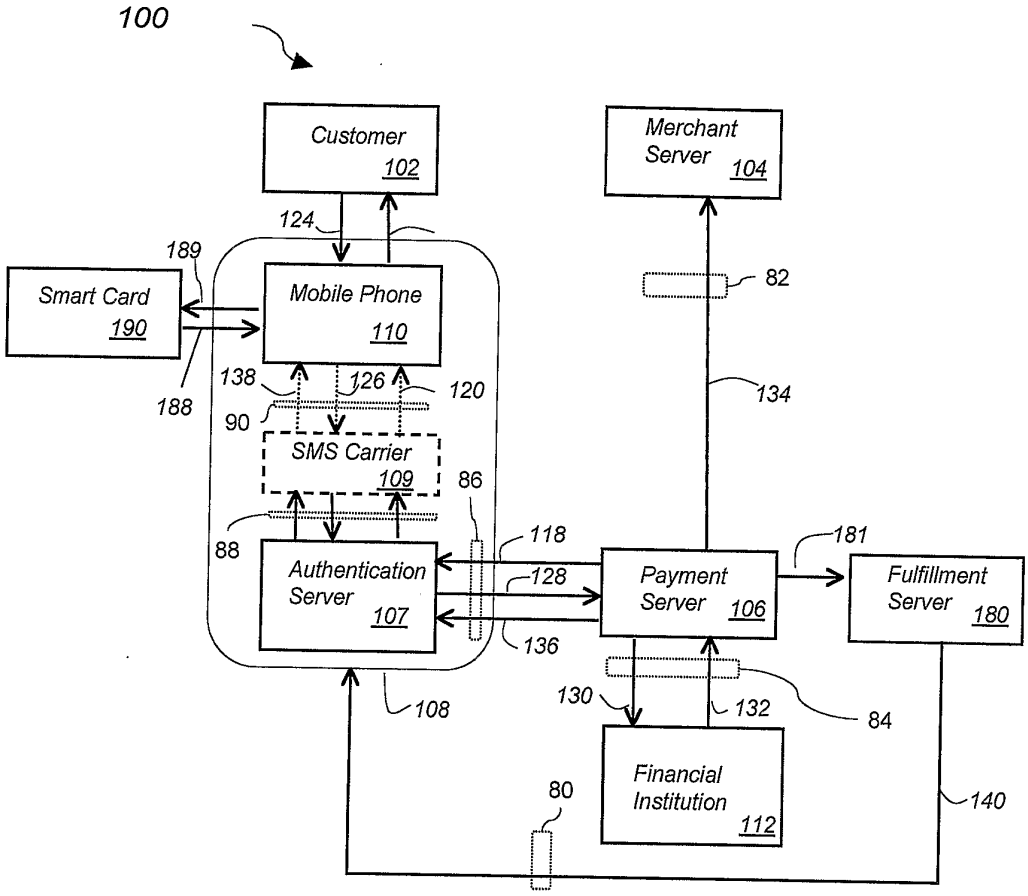

100
Customer 102
Merchant Server 104
124
189
Smart Card 190
Mobile Phone 110
82
138
126
120
188
90
SMS Carrier 109
134
86
88
118
181
Authentication Server 107
128
Payment Server 106
Fulfillment Server 180
136
108
130
132
84
Financial Institution 112
80
140

FIG. 4A

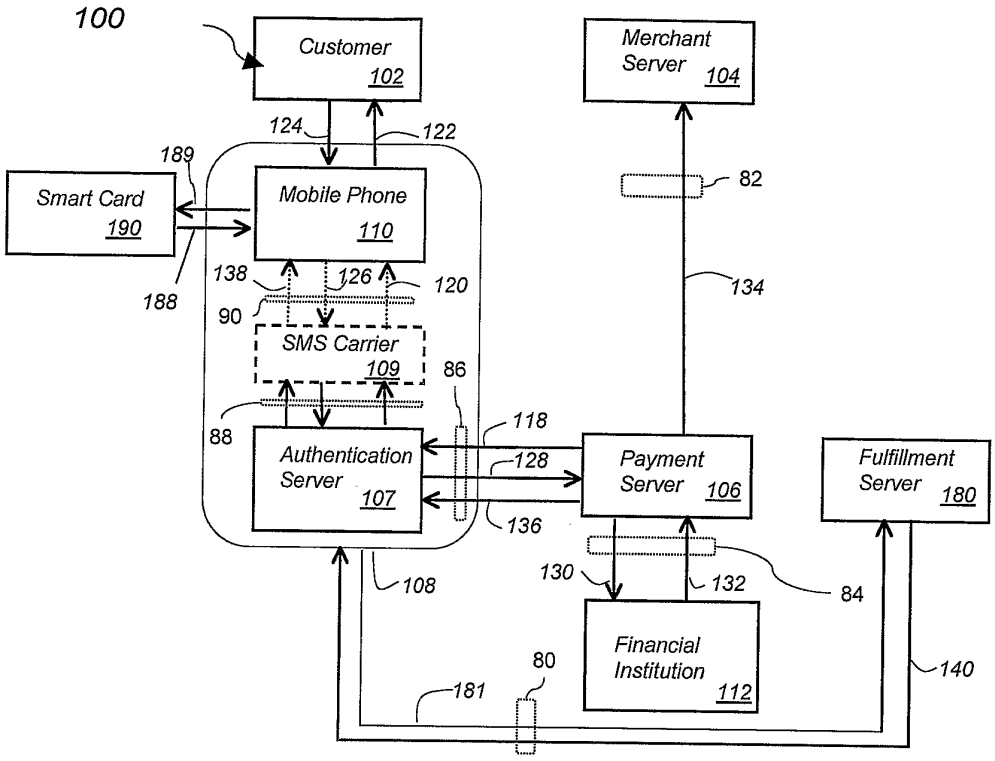

100
Customer 102
Merchant Server 104
124
122
189
Smart Card 190
Mobile Phone 110
82
138
126
120
134
188
90
SMS Carrier 109
86
88
Authentication Server 107
118
128
Payment Server 106
Fulfillment Server 180
136
130
132
84
108
Financial Institution 112
80
181
140

FIG. 4B

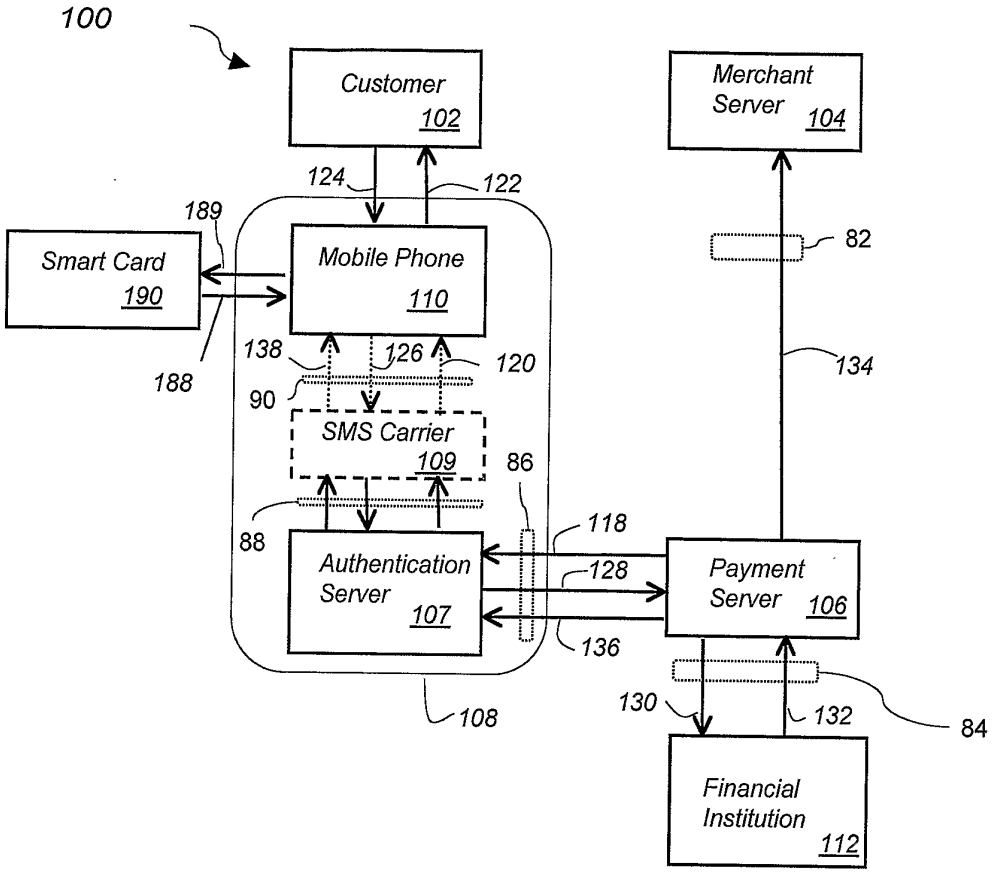

100
Customer
102
Merchant
Server
104
124
122
189
Smart Card
190
Mobile Phone
110
82
138
126
120
188
90
SMS Carrier
109
134
86
88
118
Authentication
Server
107
128
Payment
Server
106
136
130
132
84
108
Financial
Institution
112

FIG. 4C

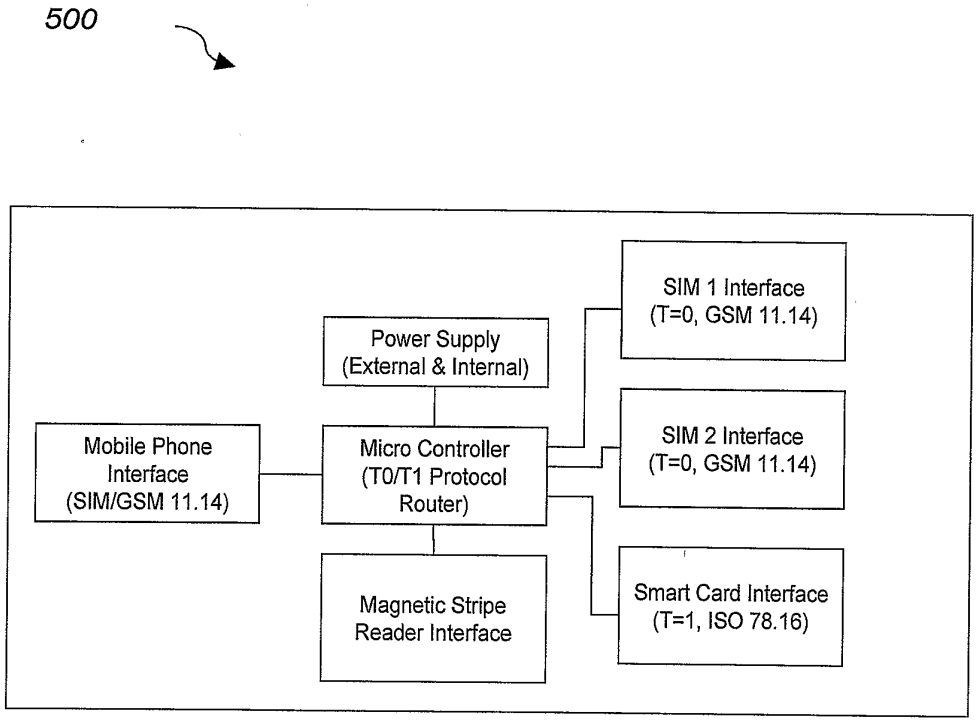

500
SIM 1 Interface
(T=0, GSM 11.14)
Power Supply
(External & Internal)
SIM 2 Interface
(T=0, GSM 11.14)
Mobile Phone
Interface
(SIM/GSM 11.14)
Micro Controller
(T0/T1 Protocol
Router)
Smart Card Interface
(T=1, ISO 78.16)
Magnetic Stripe
Reader Interface

FIG. 5

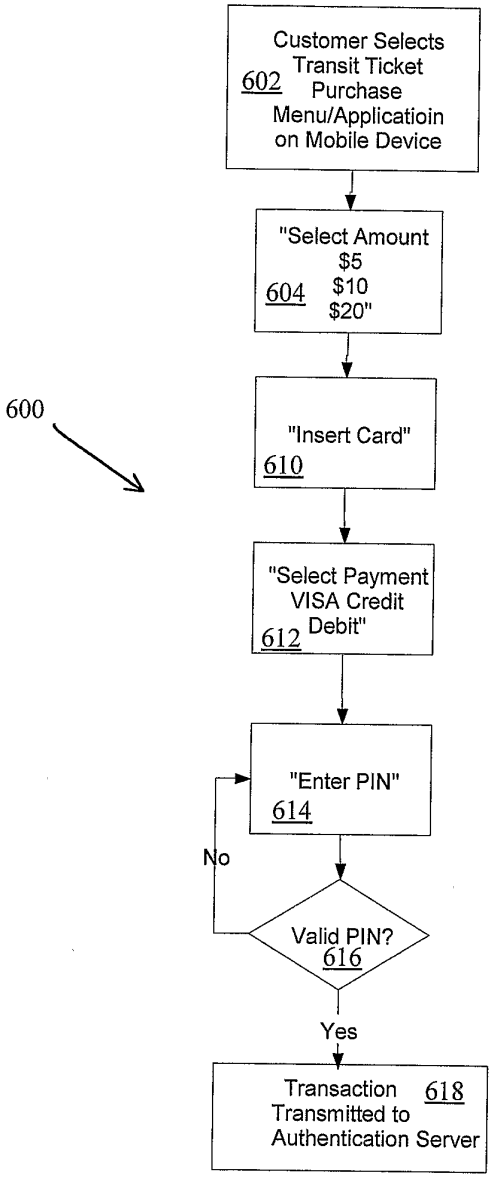
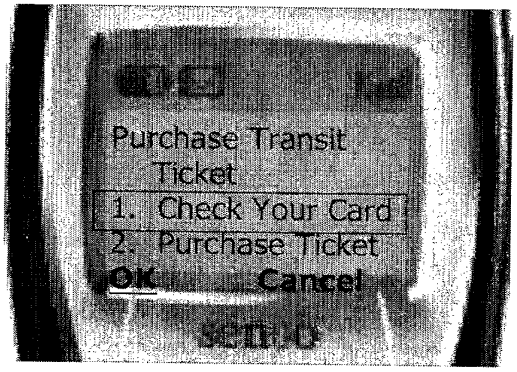

600
Customer Selects Transit Ticket Purchase Menu/Applicatioin on Mobile Device
602
"Select Amount $5 $10 $20"
604
"Insert Card"
610
"Select Payment VISA Credit Debit"
612
"Enter PIN"
614
No
Valid PIN?
616
Yes
Transaction Transmitted to Authentication Server
618

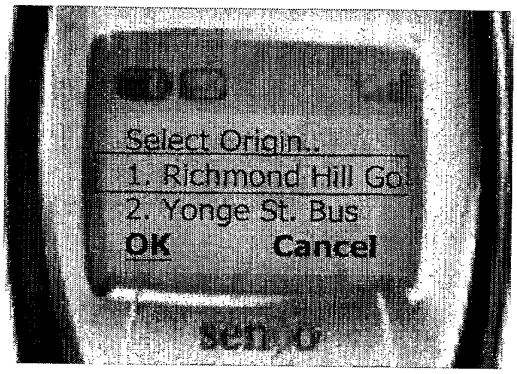
FIG. 6



602

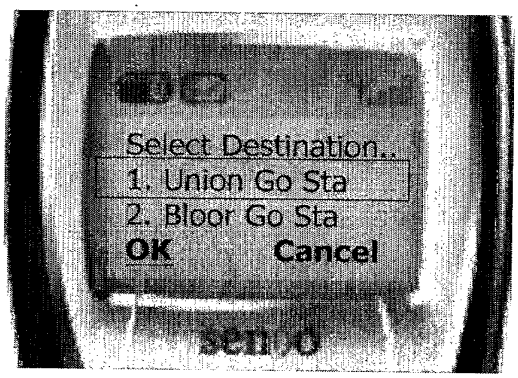
Customer chooses the Purchase Ticket option from the Phone's GO Transit Menu.

FIG. 6A



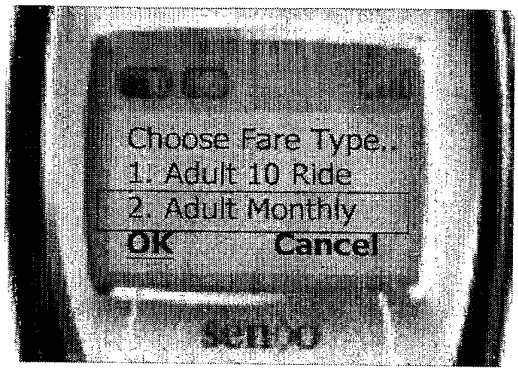
Customer Selects Origin...

FIG. 6B



Customer Selects Destination...

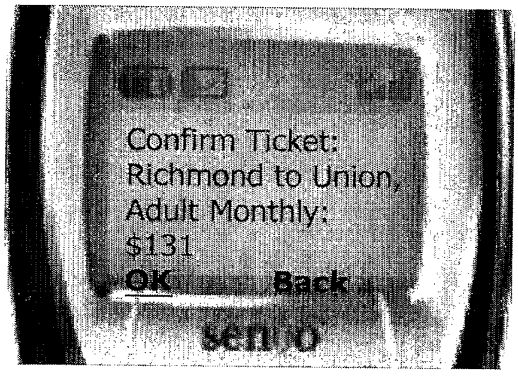
FIG. 6C



607

Customer chooses fare type...

FIG. 6D



608

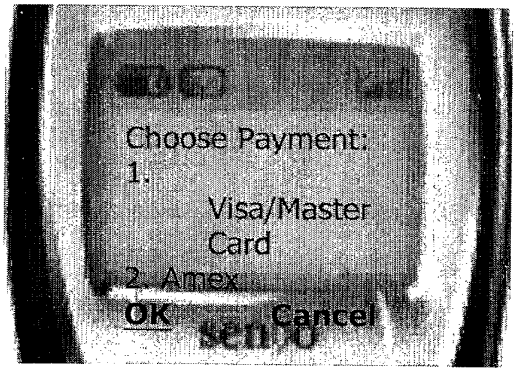
Fare is calculated and customer confirms ticket purchase

FIG. 6E

610

Customer Initiates Payment and Inserts Payment Card

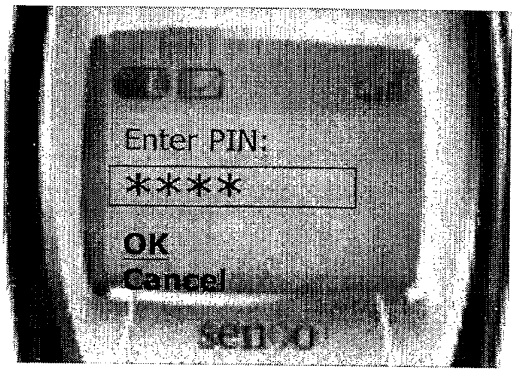
FIG. 6F



612

Customer Selects Payment Instrument on Card

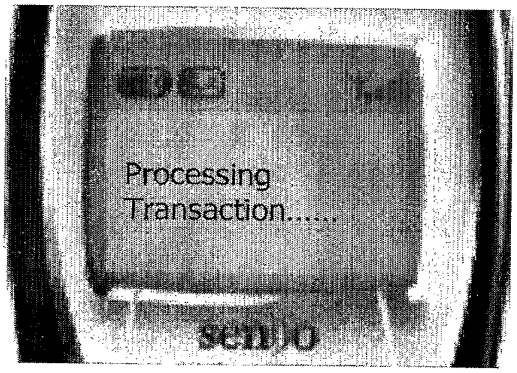
FIG. 6G



614

Customer Authenticates transaction with Personal Identification Number (PIN)

FIG. 6H



618

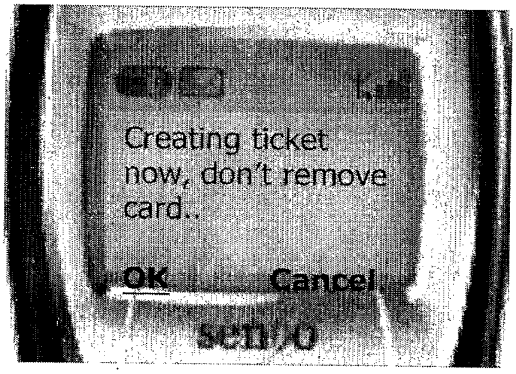
Transaction Transmitted to Authentication Server and then processed by Merchant, Financial Institution and Fulfillment Server

FIG. 6I

620

Customer presents transit card to the mobile phone

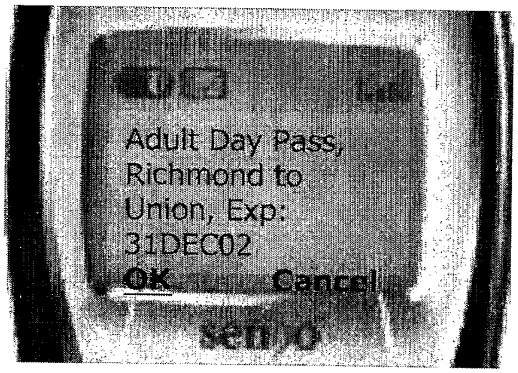
FIG. 6J



622

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).

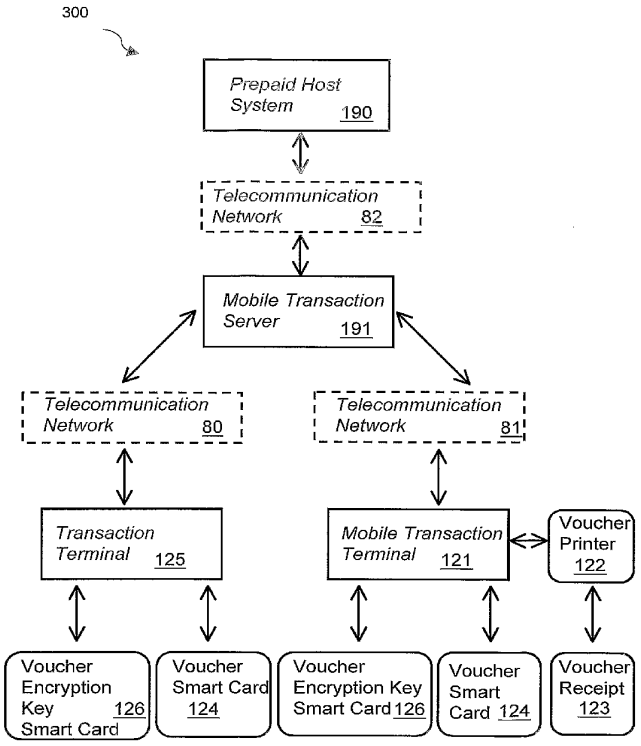
(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **BALSAN, Damien** [US/US]; 78 Melrose Street, Arlington, MA 02474 (US).

(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.

APPL-1002
APPLE INC. / Page 972 of 1892

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.

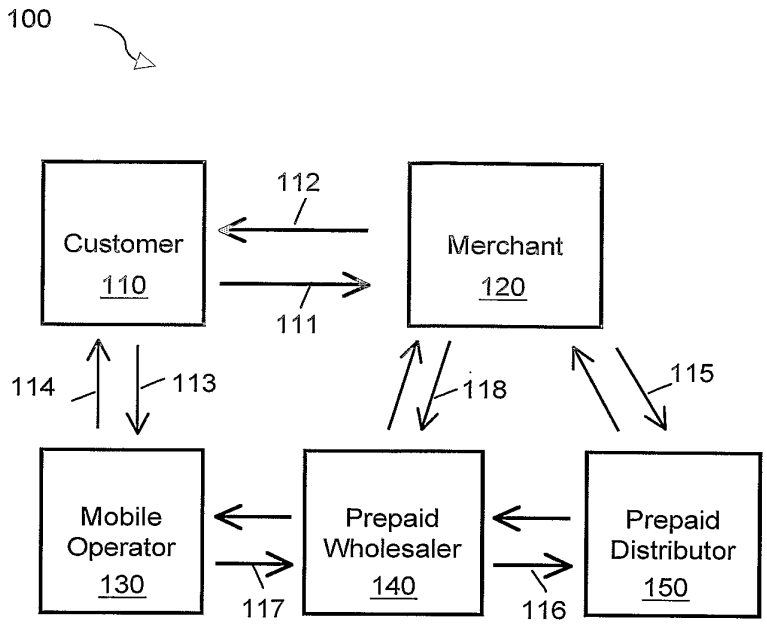


FIG. 1
(Prior Art)

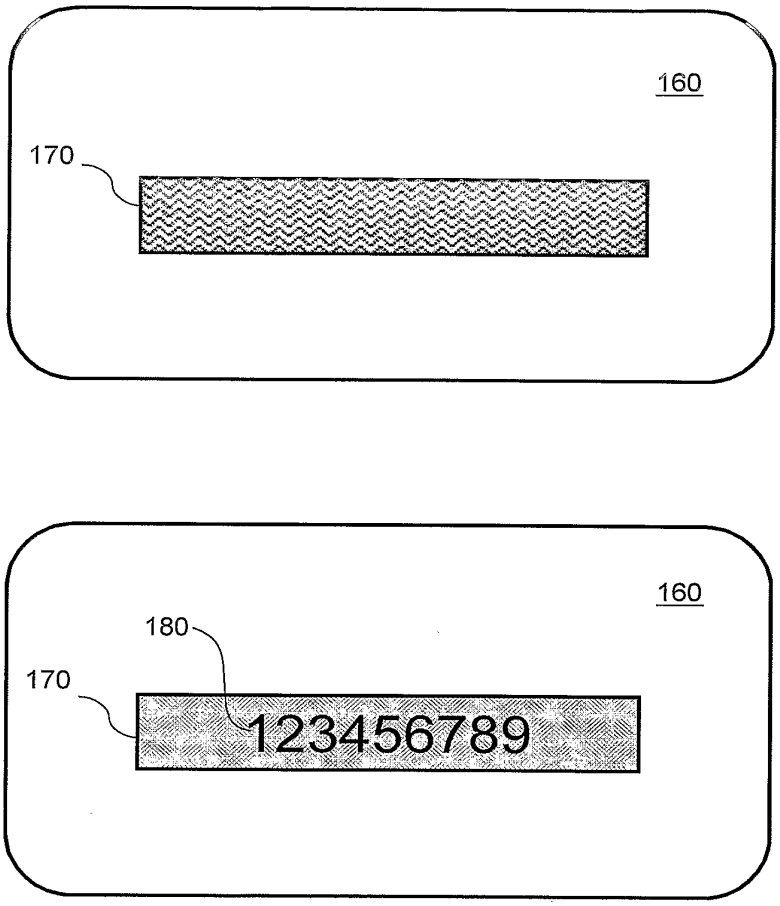


FIG. 2
(Prior Art)

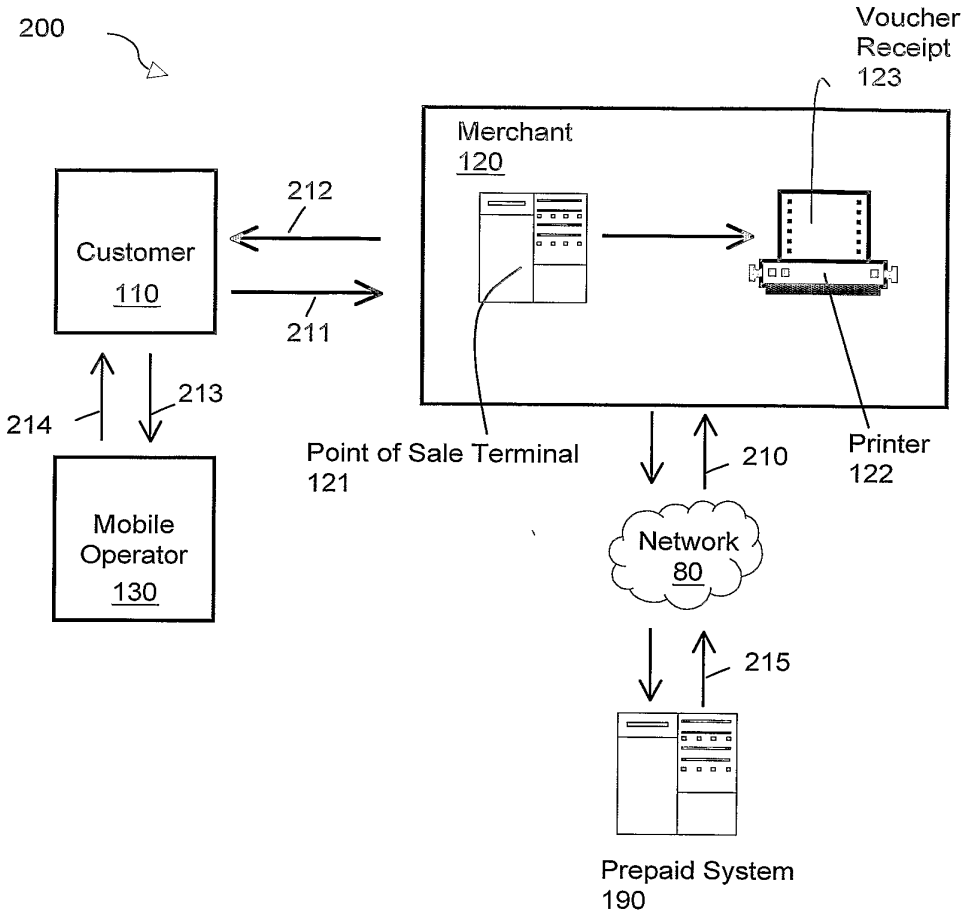


FIG. 3
(Prior Art)

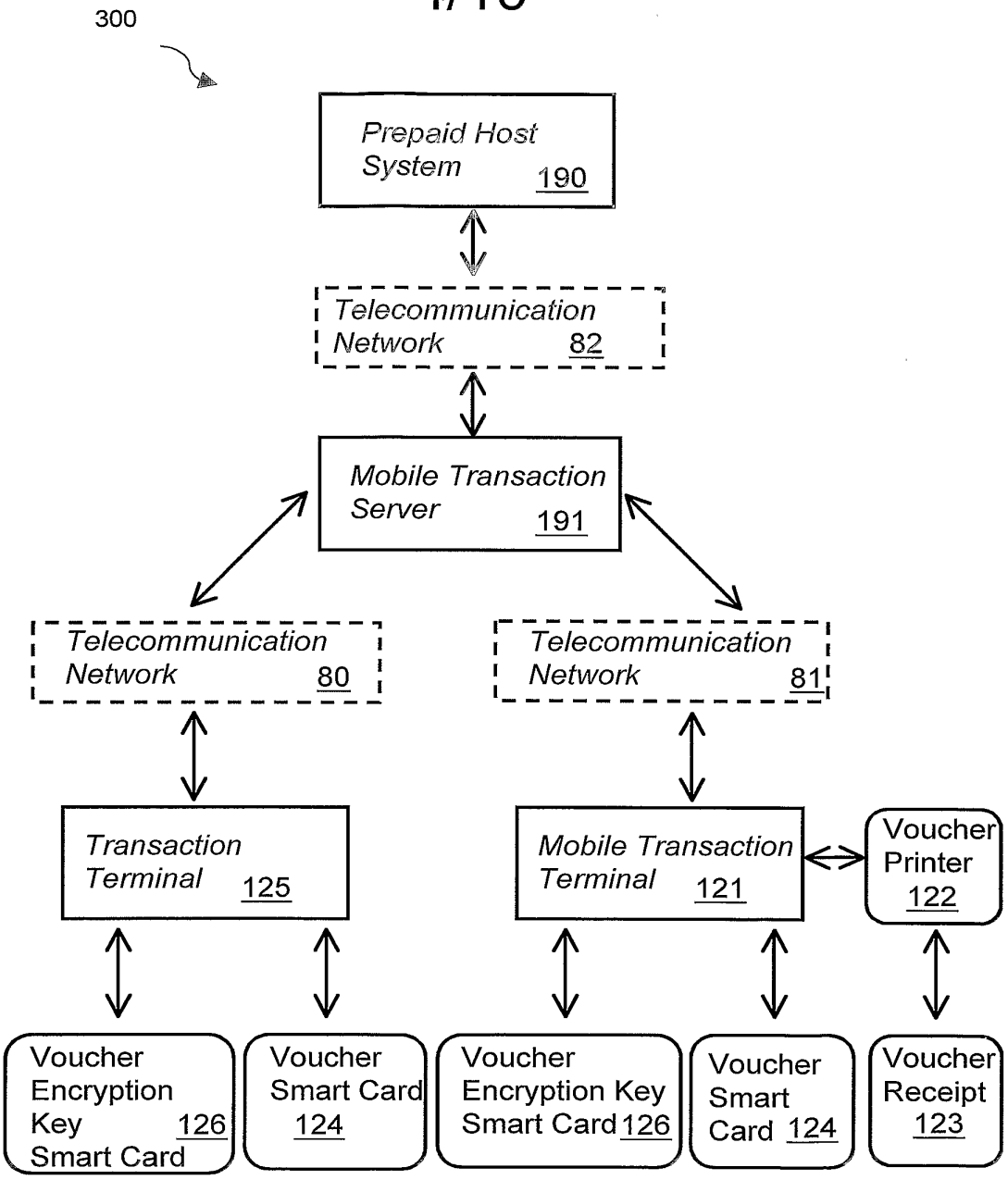

300
Prepaid Host System 190
Telecommunication Network 82
Mobile Transaction Server 191
Telecommunication Network 80
Telecommunication Network 81
Transaction Terminal 125
Mobile Transaction Terminal 121
Voucher Printer 122
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Receipt 123

FIG. 4

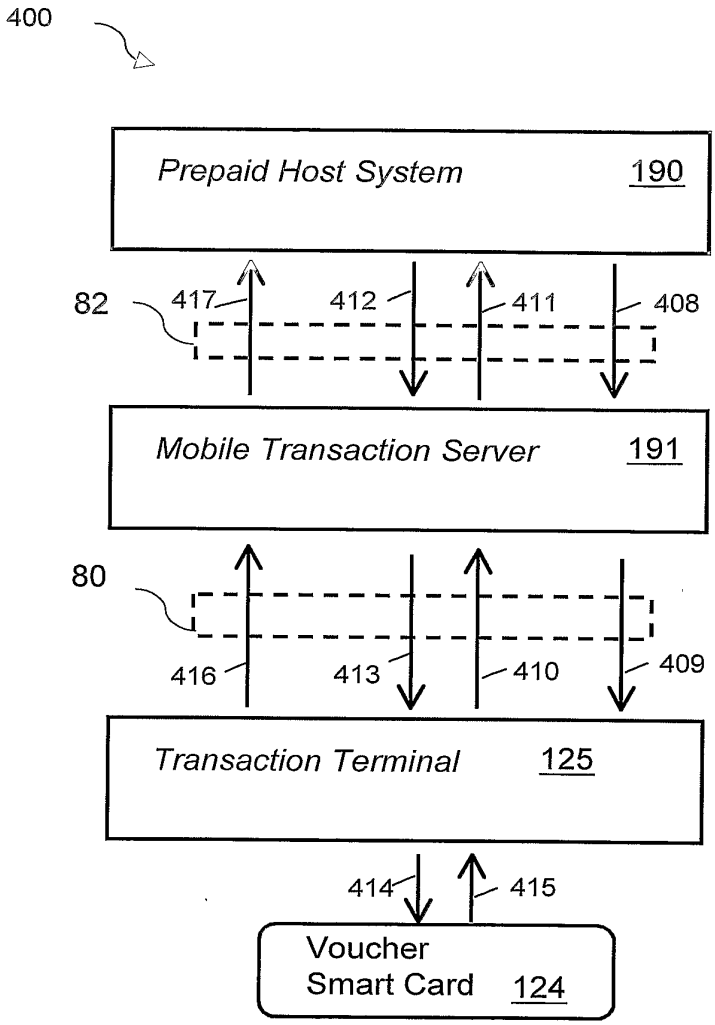

400
Prepaid Host System 190
82
417
412
411
408
Mobile Transaction Server 191
80
416
413
410
409
Transaction Terminal 125
414
415
Voucher
Smart Card 124

FIG. 5

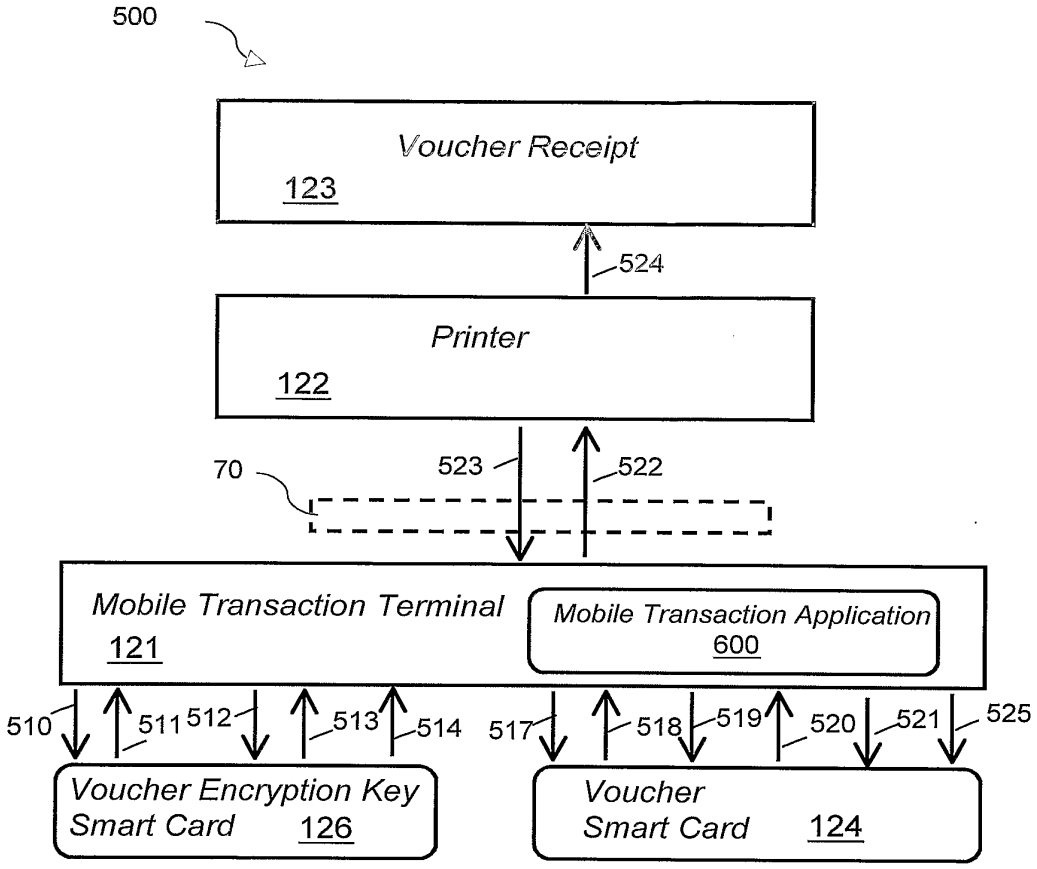

500
Voucher Receipt
123
524
Printer
122
70
523
522
Mobile Transaction Terminal
121
Mobile Transaction Application
600
510
511
512
513
514
517
518
519
520
521
525
Voucher Encryption Key
Smart Card
126
Voucher
Smart Card
124

FIG. 6

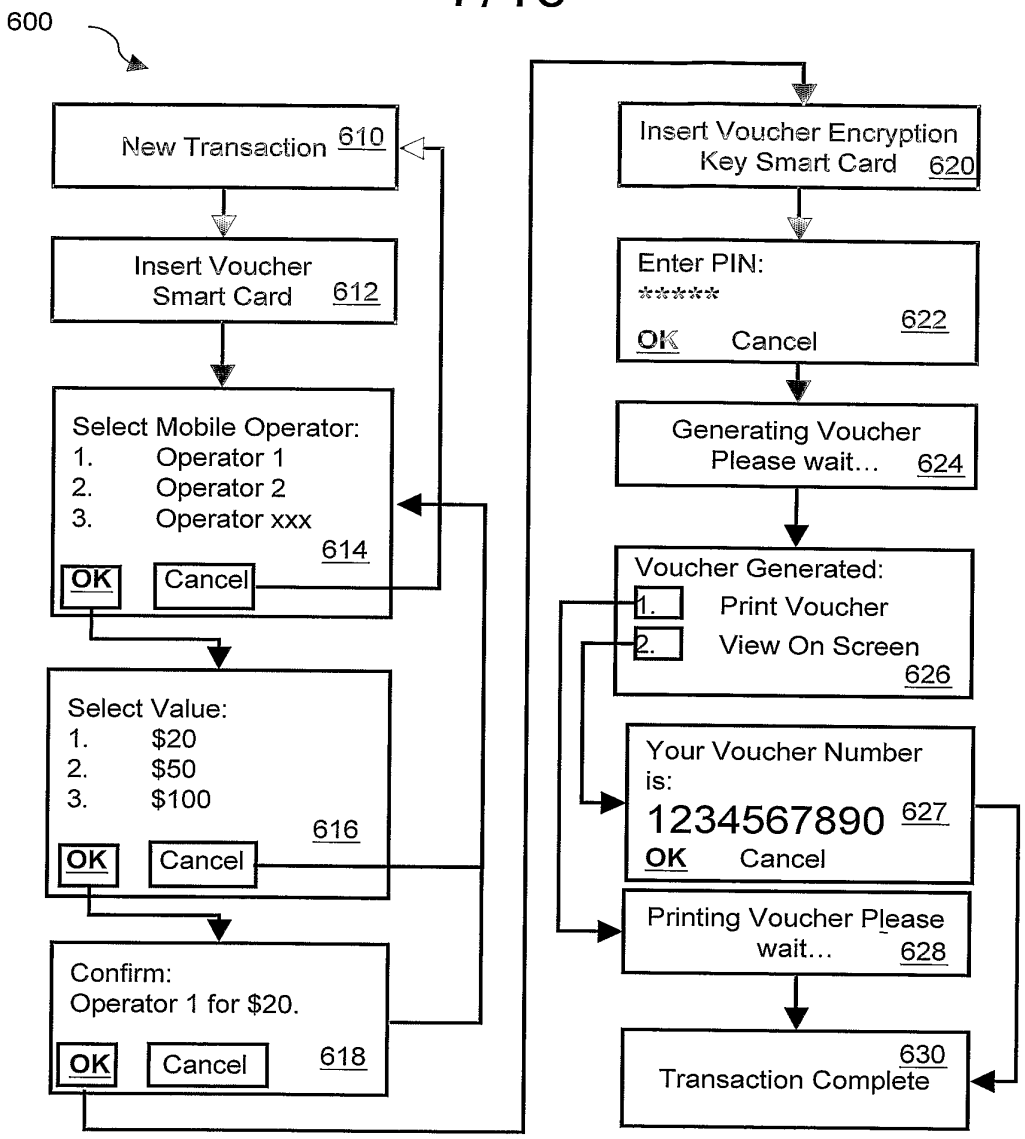

600
New Transaction 610
Insert Voucher Smart Card 612
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
614
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
616
OK
Cancel
Confirm:
Operator 1 for $20.
OK
Cancel
618
Insert Voucher Encryption Key Smart Card 620
Enter PIN:
******
622
OK
Cancel
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

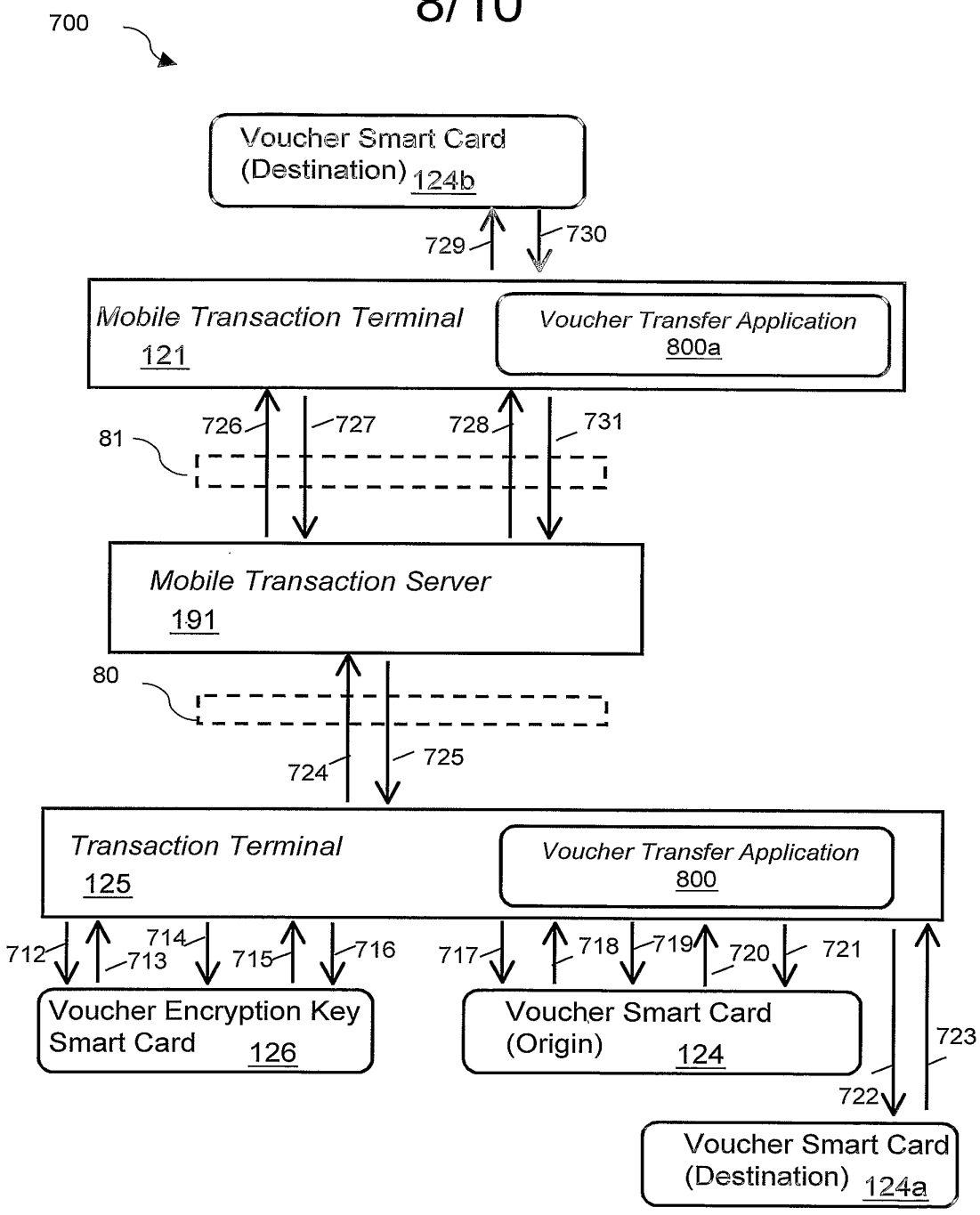

700
Voucher Smart Card (Destination) 124b
729
730
Mobile Transaction Terminal 121
Voucher Transfer Application 800a
81
726
727
728
731
Mobile Transaction Server 191
80
724
725
Transaction Terminal 125
Voucher Transfer Application 800
712
713
714
715
716
717
718
719
720
721
723
722
Voucher Encryption Key Smart Card 126
Voucher Smart Card (Origin) 124
Voucher Smart Card (Destination) 124a

FIG. 8

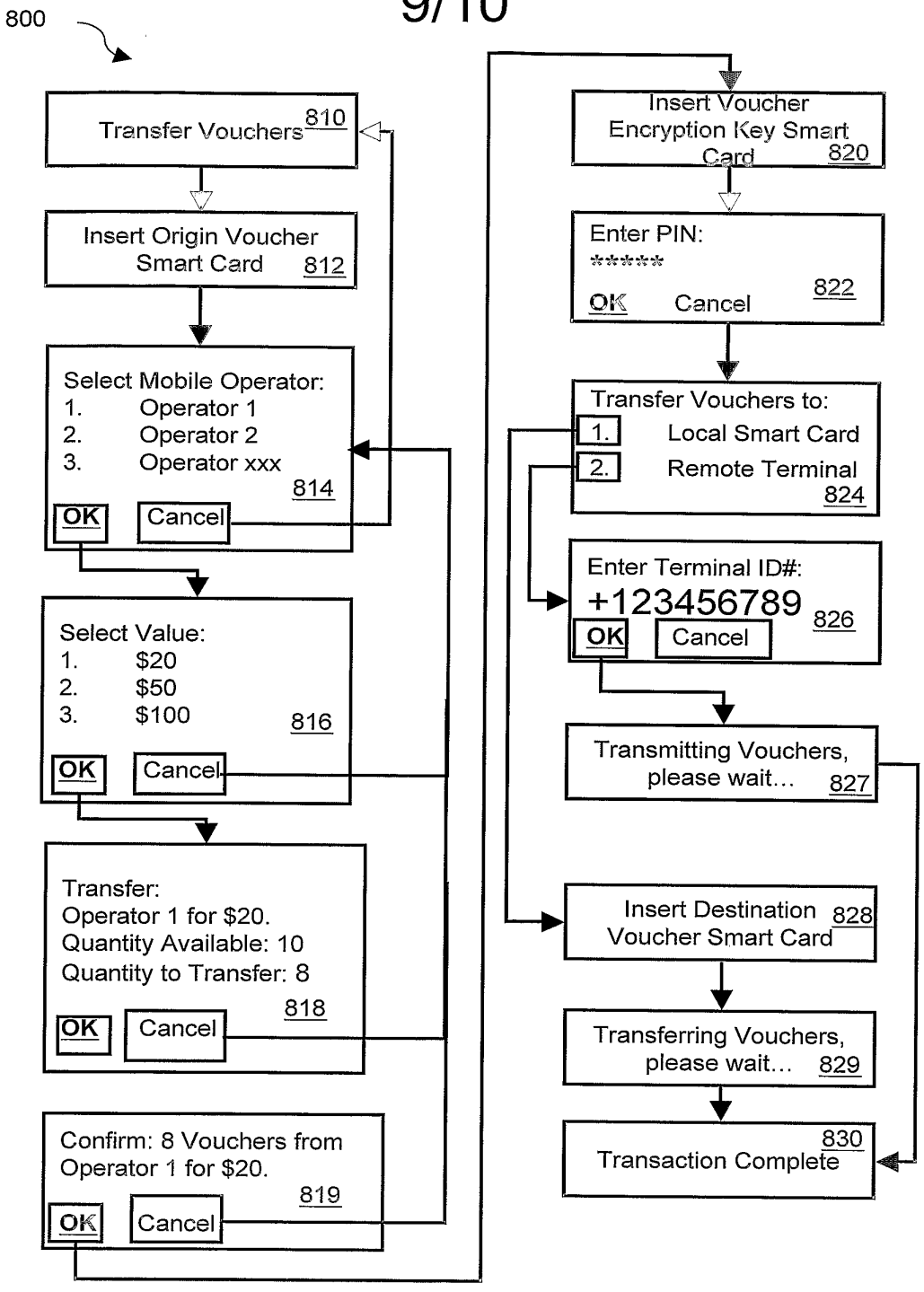

800
Transfer Vouchers 810
Insert Origin Voucher Smart Card 812
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
814
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
816
OK
Cancel
Transfer:
Operator 1 for $20.
Quantity Available: 10
Quantity to Transfer: 8
818
OK
Cancel
Confirm: 8 Vouchers 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

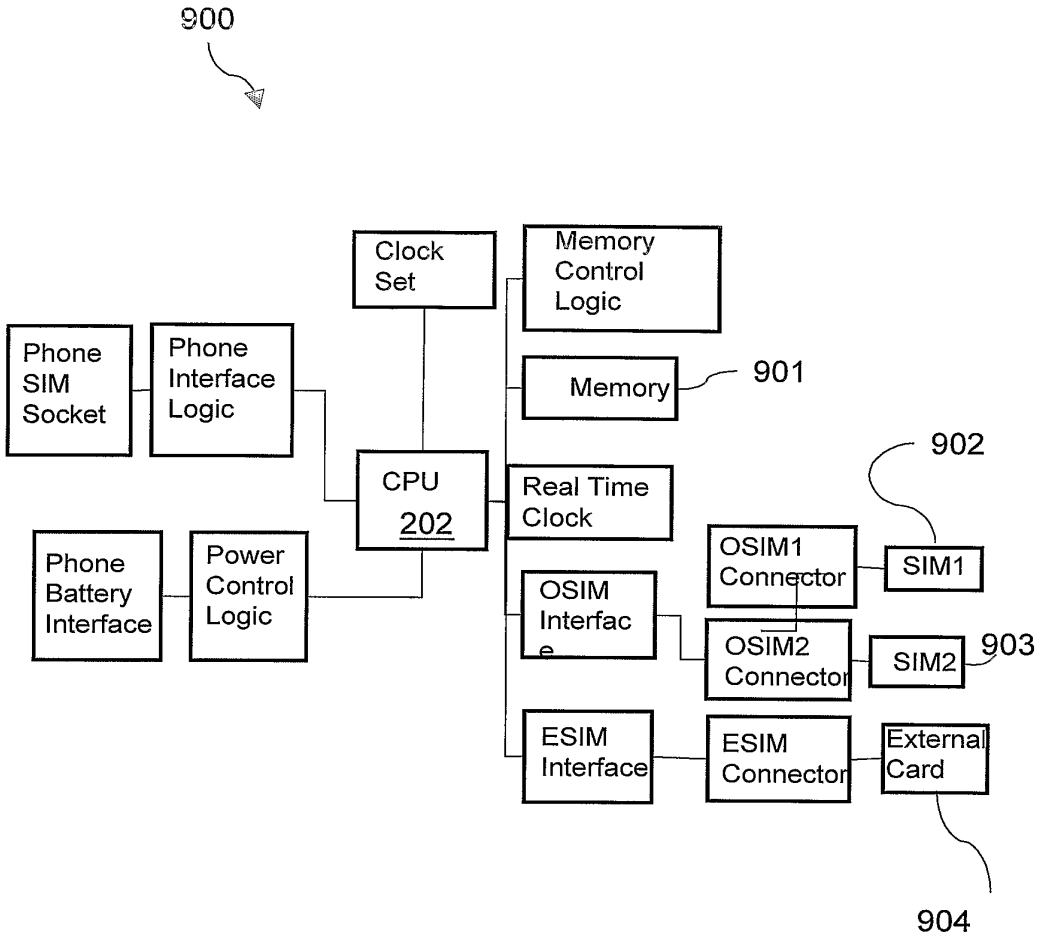

900
Clock Set
Memory Control Logic
Phone SIM Socket
Phone Interface Logic
Memory
901
902
CPU 202
Real Time Clock
Phone Battery Interface
Power Control Logic
OSIM1 Connector
SIM1
OSIM Interfac e
OSIM2 Connector
SIM2
903
ESIM Interface
ESIM Connector
External Card
904

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).

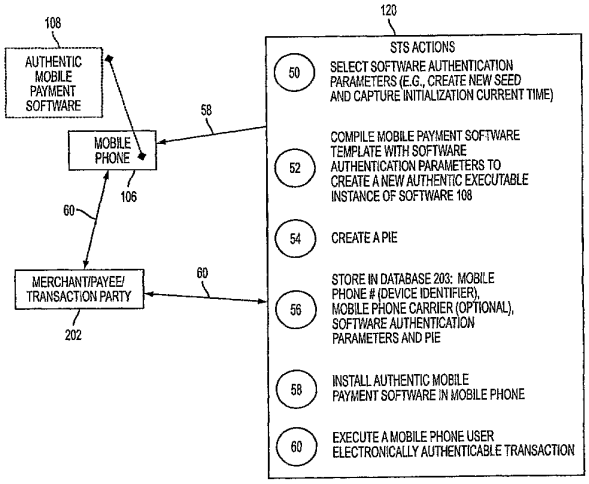
(74) Agent: **SHEIKERZ, Mehdi, D.**; Staas & Halsey LLP, Suite 700, 1201 New York Avenue, Washington, DC 20005 (US).

(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.

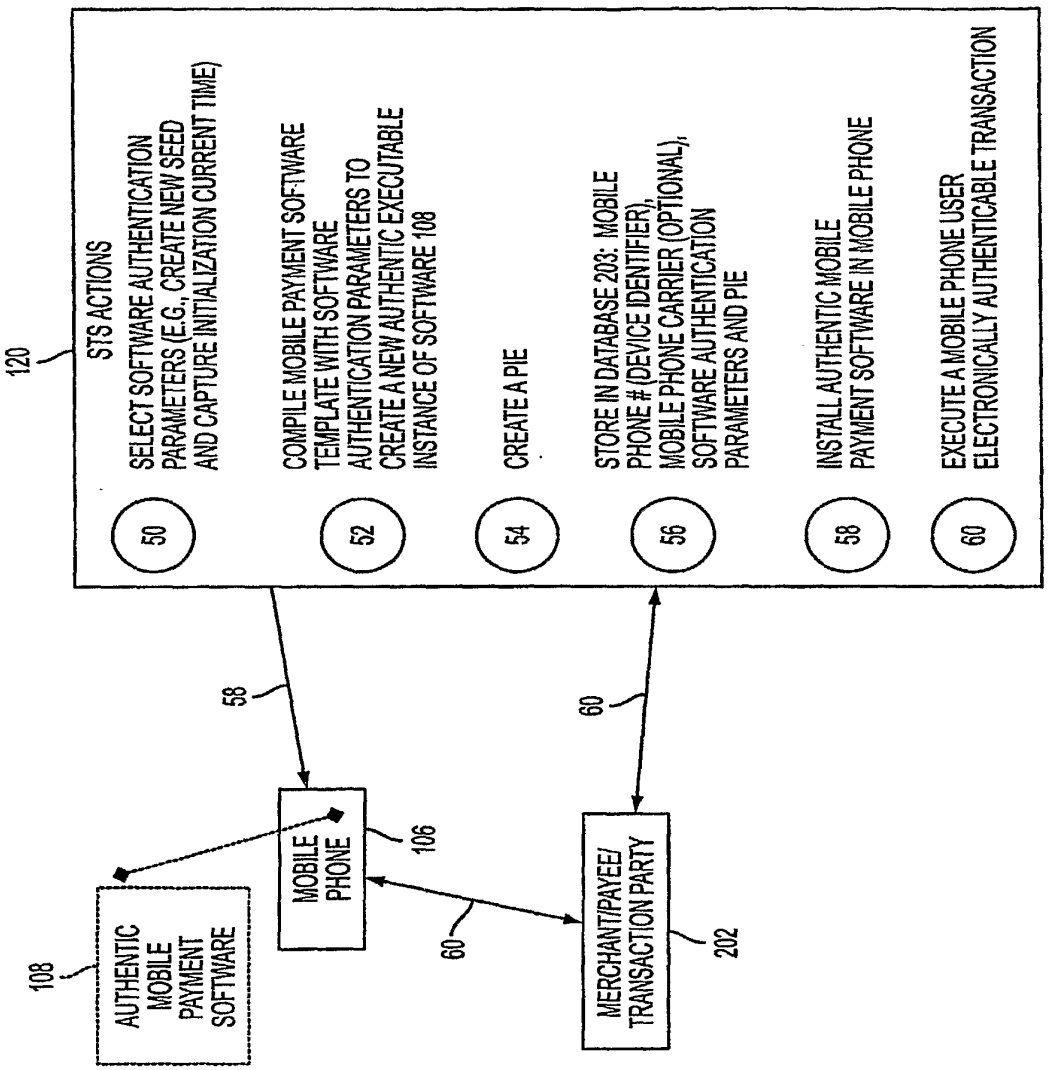

120
STS ACTIONS
50
SELECT SOFTWARE AUTHENTICATION PARAMETERS (E.G., CREATE NEW SEED AND CAPTURE INITIALIZATION CURRENT TIME)
52
COMPILE MOBILE PAYMENT SOFTWARE TEMPLATE WITH SOFTWARE AUTHENTICATION PARAMETERS TO CREATE A NEW AUTHENTIC EXECUTABLE INSTANCE OF SOFTWARE 108
54
CREATE A PIE
56
STORE IN DATABASE 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

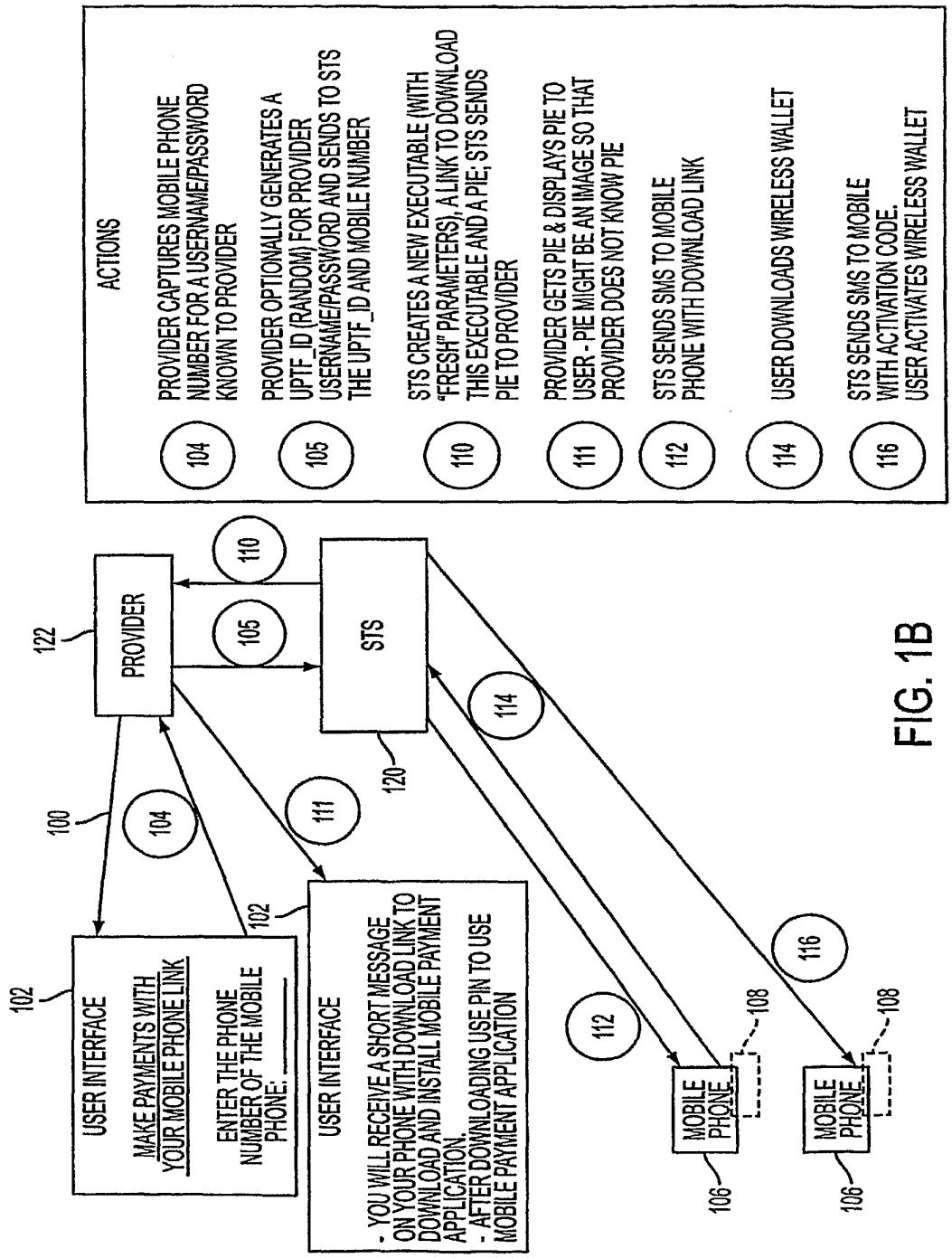

ACTIONS
104 PROVIDER CAPTURES MOBILE PHONE NUMBER FOR A USERNAME/PASSWORD KNOWN TO PROVIDER
105 PROVIDER OPTIONALLY GENERATES A UPTF_ID (RANDOM) FOR PROVIDER USERNAME/PASSWORD AND SENDS TO STS THE UPTF_ID AND MOBILE NUMBER
110 STS CREATES A NEW EXECUTABLE (WITH "FRESH" PARAMETERS), A LINK TO DOWNLOAD 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
122 PROVIDER
STS
120
100
102
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
106
108

FIG. 1B

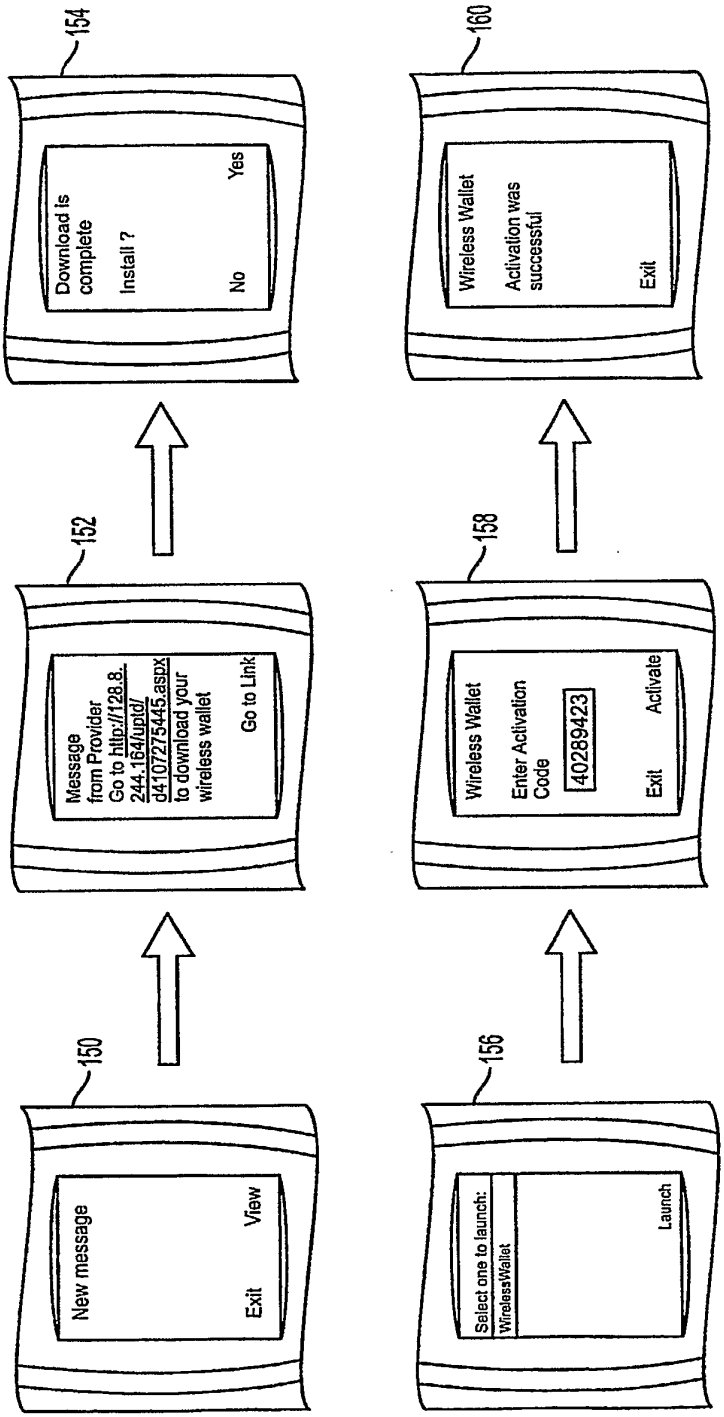

154
Download is complete
Install ?
Yes
No
160
Wireless Wallet
Activation was successful
Exit
152
Message from Provider
Go to http://128.8.244.164/uptd/d4107275445.aspx to download your wireless wallet
Go to Link
158
Wireless Wallet
Enter Activation Code
40289423
Exit
Activate
150
New message
Exit
View
156
Select one to launch:
WirelessWallet
Launch

FIG. 1C

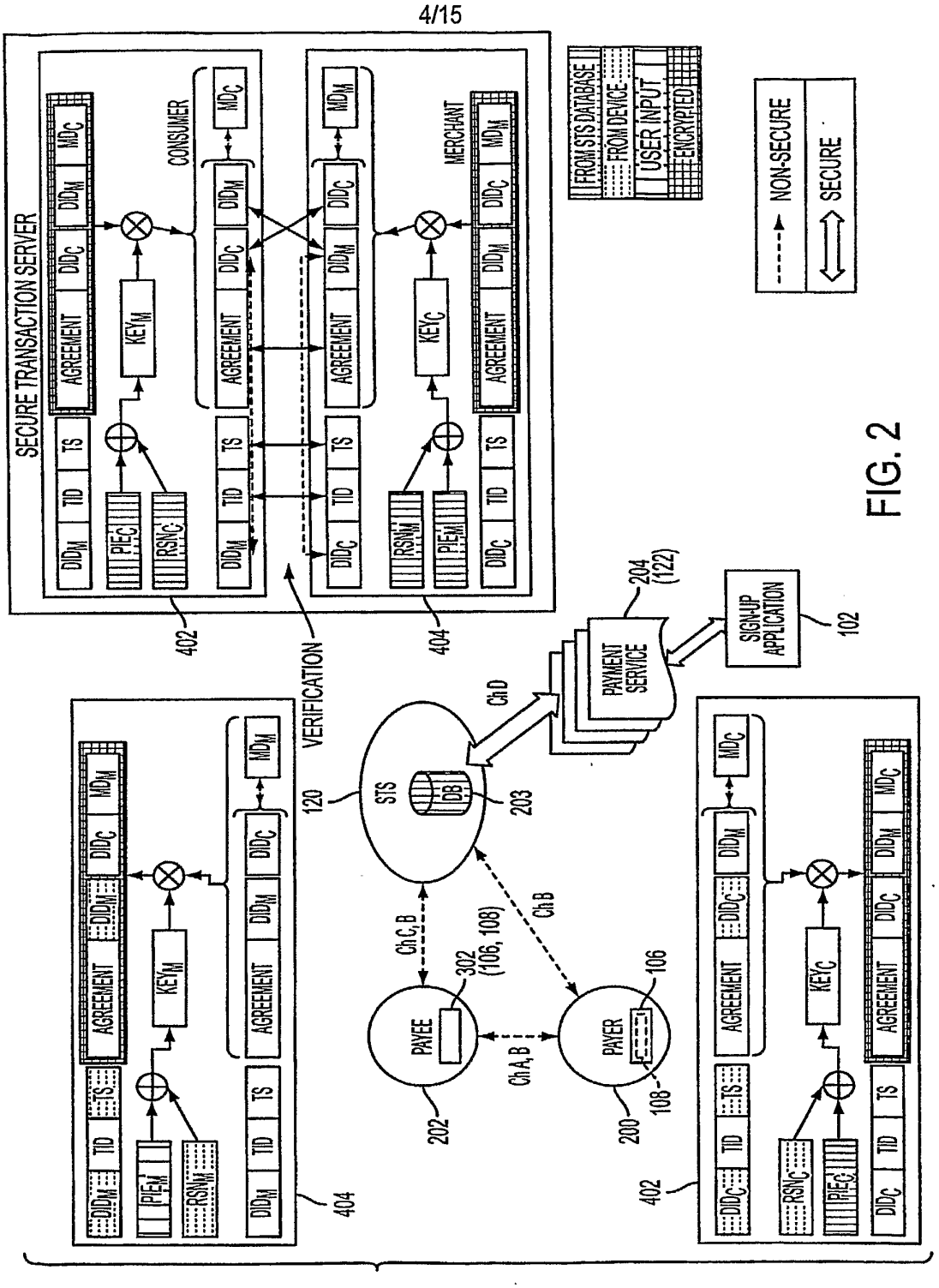

SECURE TRANSACTION SERVER
CONSUMER
MERCHANT
AGREEMENT
KEY$_M$
KEY$_C$
DID$_M$
DID$_C$
MD$_C$
MD$_M$
TID
TS
PIE$_C$
PIE$_M$
RSN$_C$
RSN$_M$
402
404
VERIFICATION
120
STS
DB
203
ChD
PAYMENT SERVICE
204 (122)
SIGN-UP APPLICATION
102
ChC, B
ChB
ChA, B
PAYEE
302 (106, 108)
PAYER
106
108
202
200
FROM STS DATABASE
FROM DEVICE
USER INPUT ENCRYPTED
NON-SECURE
SECURE

FIG. 2

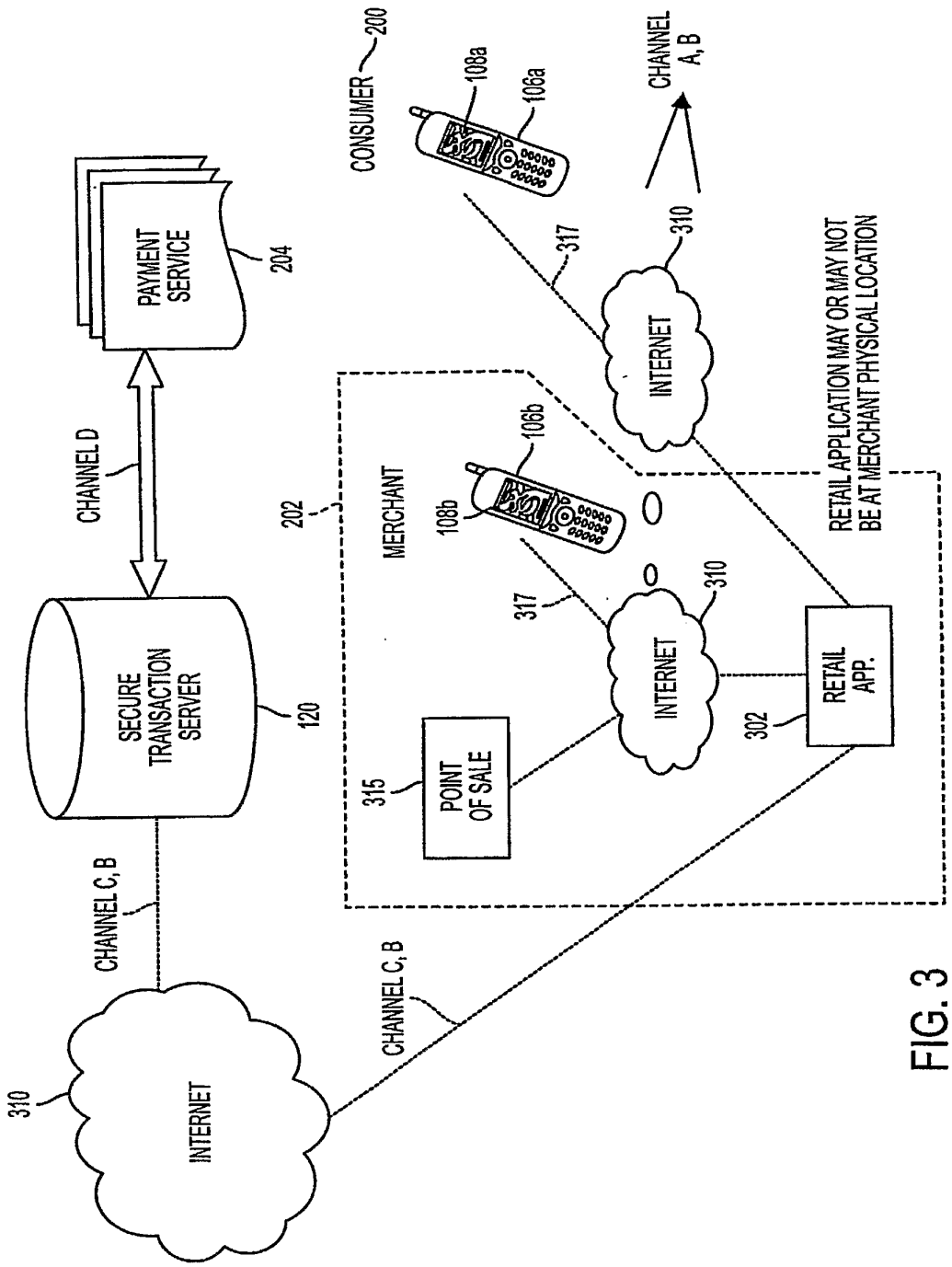
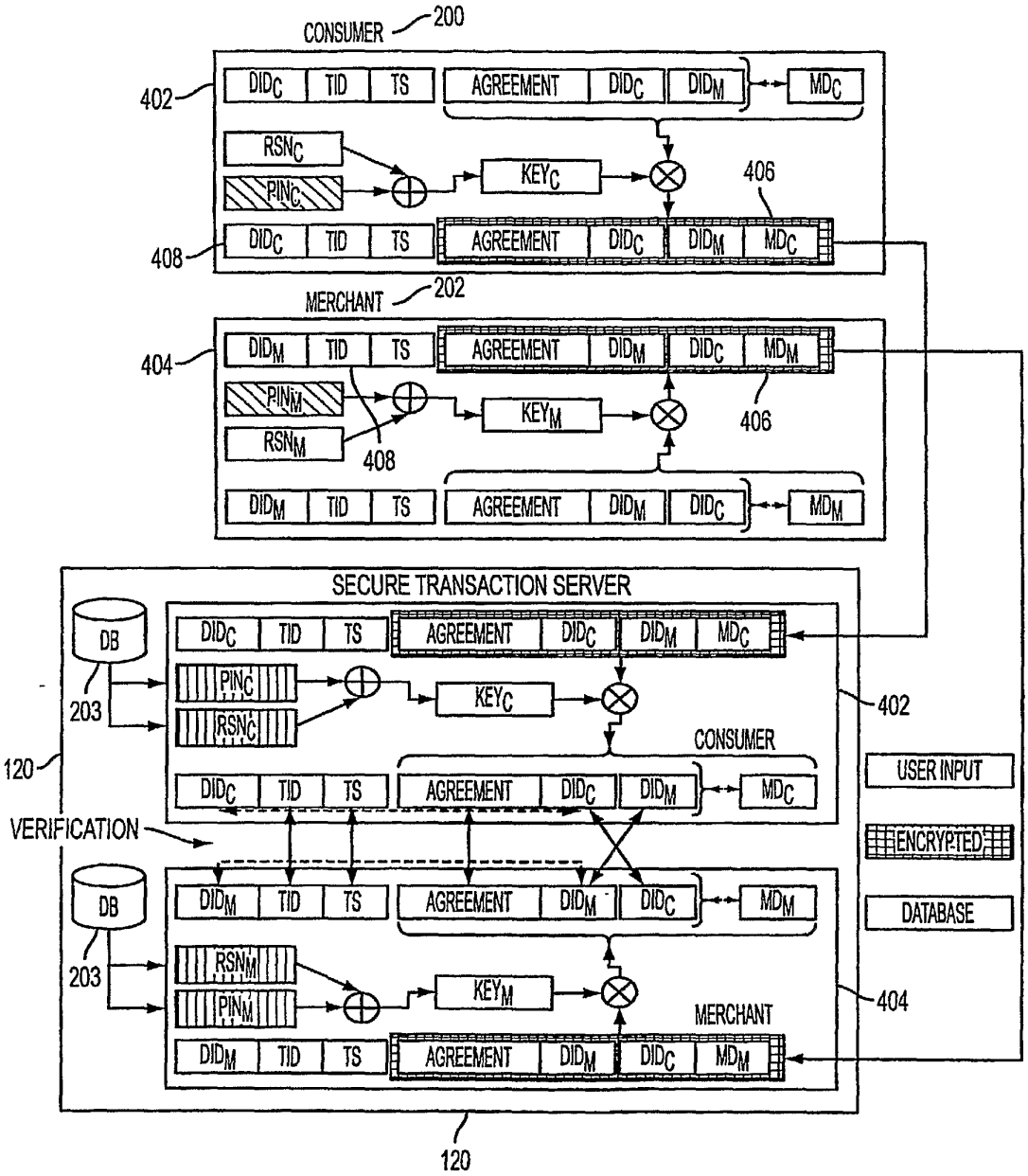

CONSUMER
200
108a
106a
CHANNEL A, B
317
310
INTERNET
PAYMENT SERVICE
204
CHANNEL D
MERCHANT
202
106b
108b
RETAIL APPLICATION MAY OR MAY NOT BE AT MERCHANT PHYSICAL LOCATION
317
310
INTERNET
SECURE TRANSACTION SERVER
120
RETAIL APP.
302
315
POINT OF SALE
CHANNEL C, B
CHANNEL C, B
310
INTERNET

FIG. 3



CONSUMER AND MERCHANT MESSAGE ENCRYPTION AND SECURE TRANSACTION SERVER PROCESSING

FIG. 4

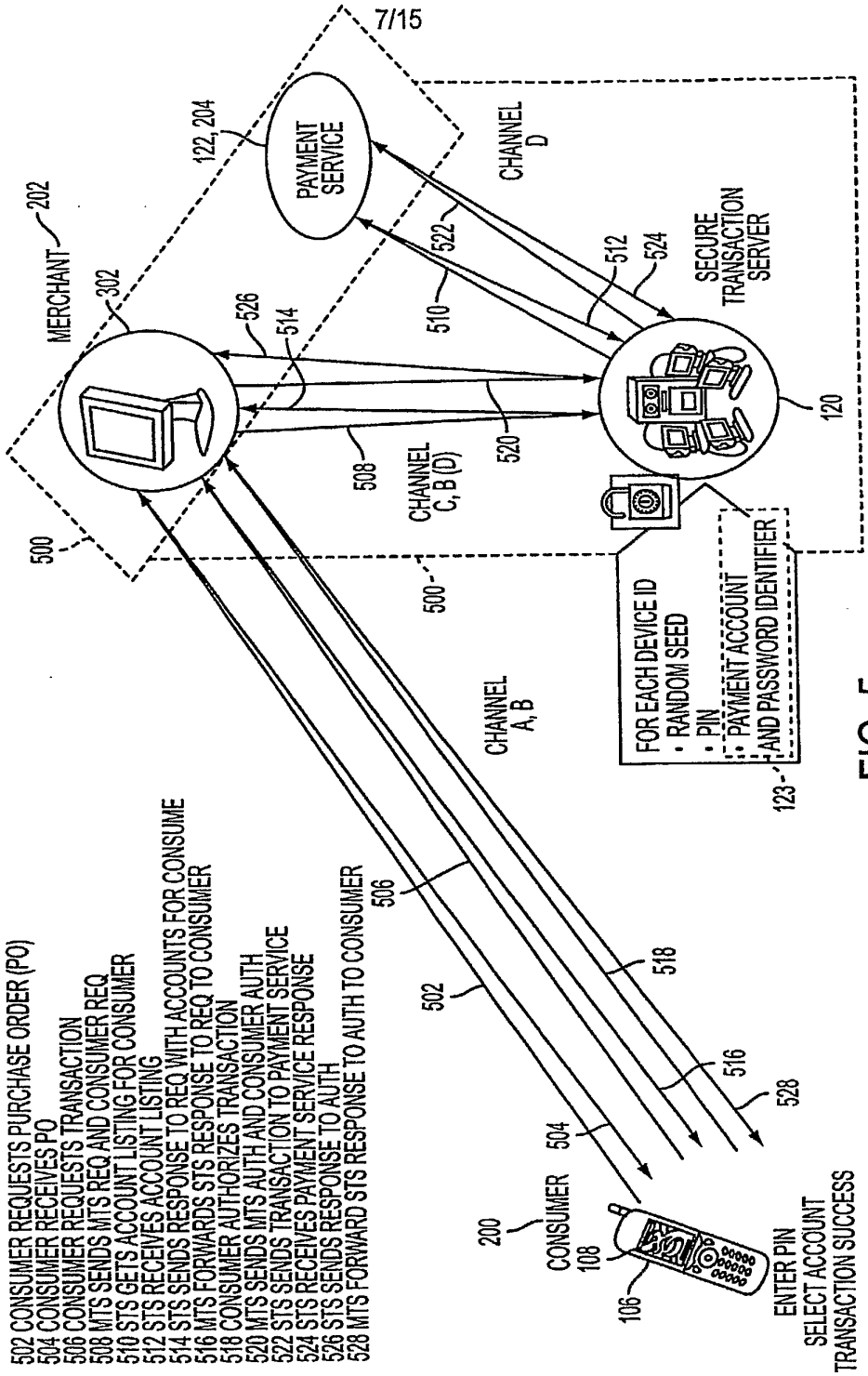

7/15
A COMPLETE TRANSACTION
502 CONSUMER REQUESTS PURCHASE ORDER (PO)
504 CONSUMER RECEIVES PO
506 CONSUMER REQUESTS TRANSACTION
508 MTS SENDS MTS REQ AND CONSUMER REQ
510 STS GETS ACCOUNT LISTING FOR CONSUMER
512 STS RECEIVES ACCOUNT LISTING
514 STS SENDS RESPONSE TO REQ WITH ACCOUNTS FOR CONSUME
516 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
ENTER PIN
SELECT ACCOUNT
TRANSACTION SUCCESS
CONSUMER
200
108
106
MERCHANT
202
302
500
122, 204
PAYMENT SERVICE
SECURE TRANSACTION SERVER
120
CHANNEL A, B
CHANNEL C, B (D)
CHANNEL D
FOR EACH DEVICE ID
• RANDOM SEED
• PIN
• PAYMENT ACCOUNT
AND PASSWORD IDENTIFIER
123

FIG. 5

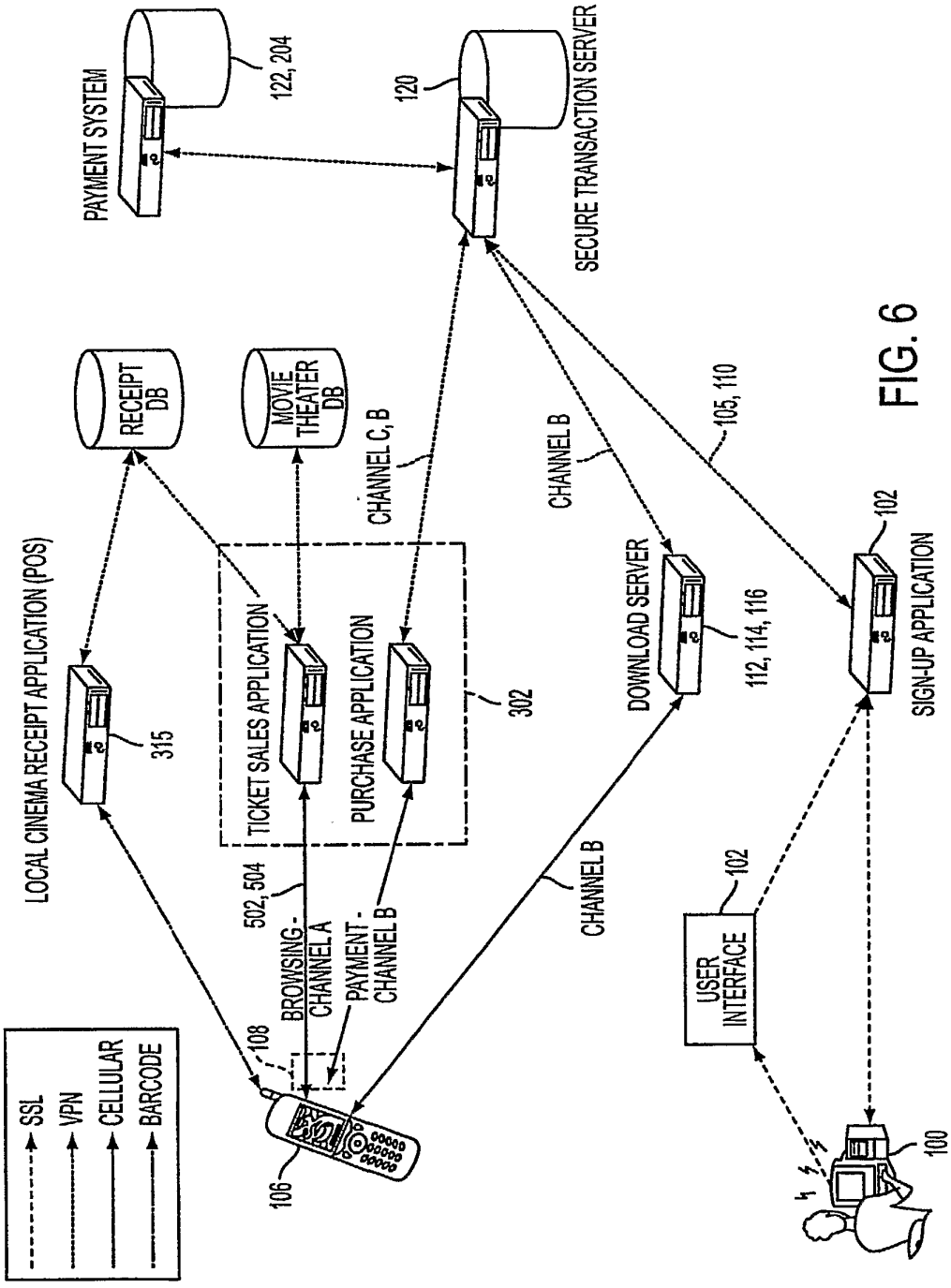

PAYMENT SYSTEM
122, 204
120
SECURE TRANSACTION SERVER
RECEIPT DB
MOVIE THEATER DB
CHANNEL C, B
CHANNEL B
105, 110
LOCAL CINEMA RECEIPT APPLICATION (POS)
315
TICKET SALES APPLICATION
PURCHASE APPLICATION
302
DOWNLOAD SERVER
112, 114, 116
102
SIGN-UP APPLICATION
502, 504
BROWSING - CHANNEL A
PAYMENT - CHANNEL B
CHANNEL B
108
106
USER INTERFACE
102
100
SSL
VPN
CELLULAR
BARCODE

FIG. 6

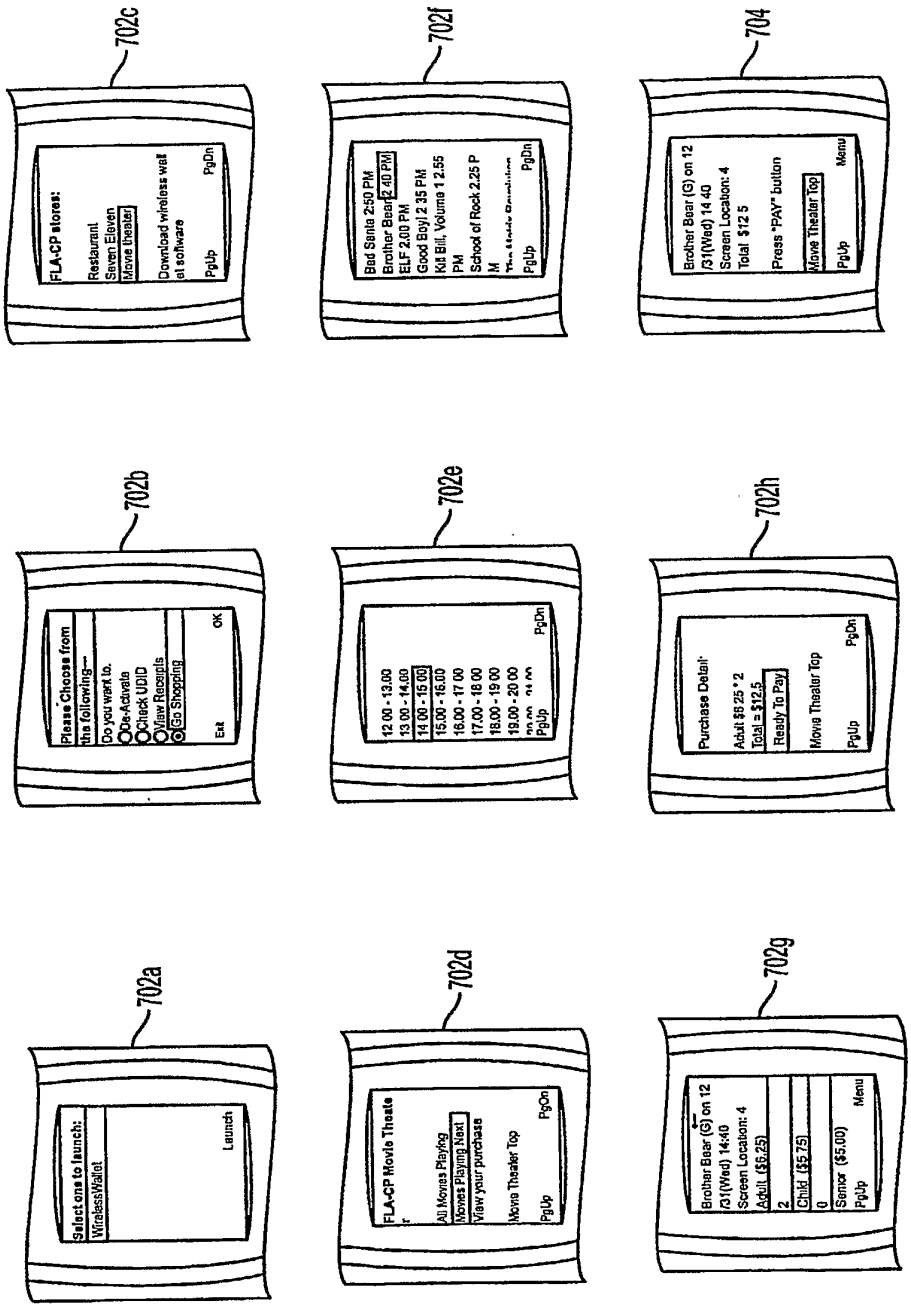

702c
FLA-CP stores:
Restaurant
Seven Eleven
Movie theater
Download wireless wall st software
PgUp
PgDn
702f
Bad Santa 2:50 PM
Brother Bear 2:40 PM
ELF 2:00 PM
Good Boy! 2:35 PM
Kill Bill, Volume 1 2:55 PM
School of Rock 2:25 P M
PgUp
PgDn
704
Brother Bear (G) on 12 /31(Wed) 14:40
Screen Location: 4
Total $12.5
Press "PAY" button
Movie Theater Top
PgUp
Menu
702b
Please Choose from the following—
Do you want to.
De-Activate
Check UDID
View Receipts
Go Shopping
Exit
OK
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

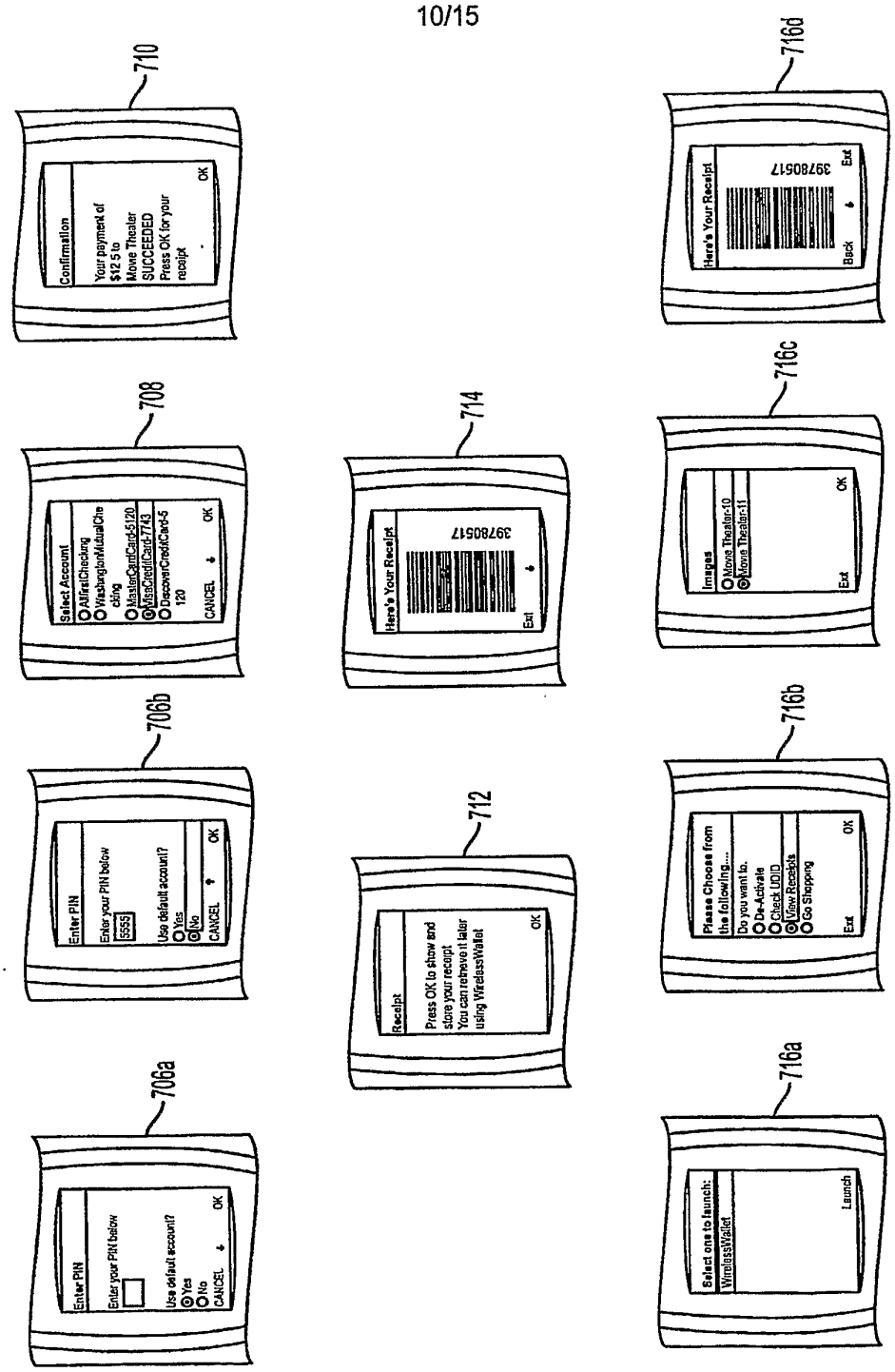

710
Confirmation
Your payment of $12.5 to Movie Theater SUCCEEDED Press OK for your receipt
OK
708
Select Account
AllfirstChecking
WashingtonMutualChecking
MasterCardCard-5120
MiscCreditCard-7743
DiscoverCreditCard-5120
CANCEL
OK
706b
Enter PIN
Enter your PIN below
5555
Use default account?
Yes
No
CANCEL
OK
706a
Enter PIN
Enter your PIN below
Use default account?
Yes
No
CANCEL
OK
714
Here's Your Receipt
39780517
Ext
712
Receipt
Press OK to show and store your receipt You can retrieve it later using WirelessWallet
OK
716d
Here's Your Receipt
39780517
Back
Ext
716c
Images
Movie Theater-10
Movie Theater-11
Ext
OK
716b
Please Choose from the following....
Do you want to.
De-Activate
Check UDID
View Receipts
Go Shopping
Ext
OK
716a
Select one to launch:
WirelessWallet
Launch

FIG. 7B

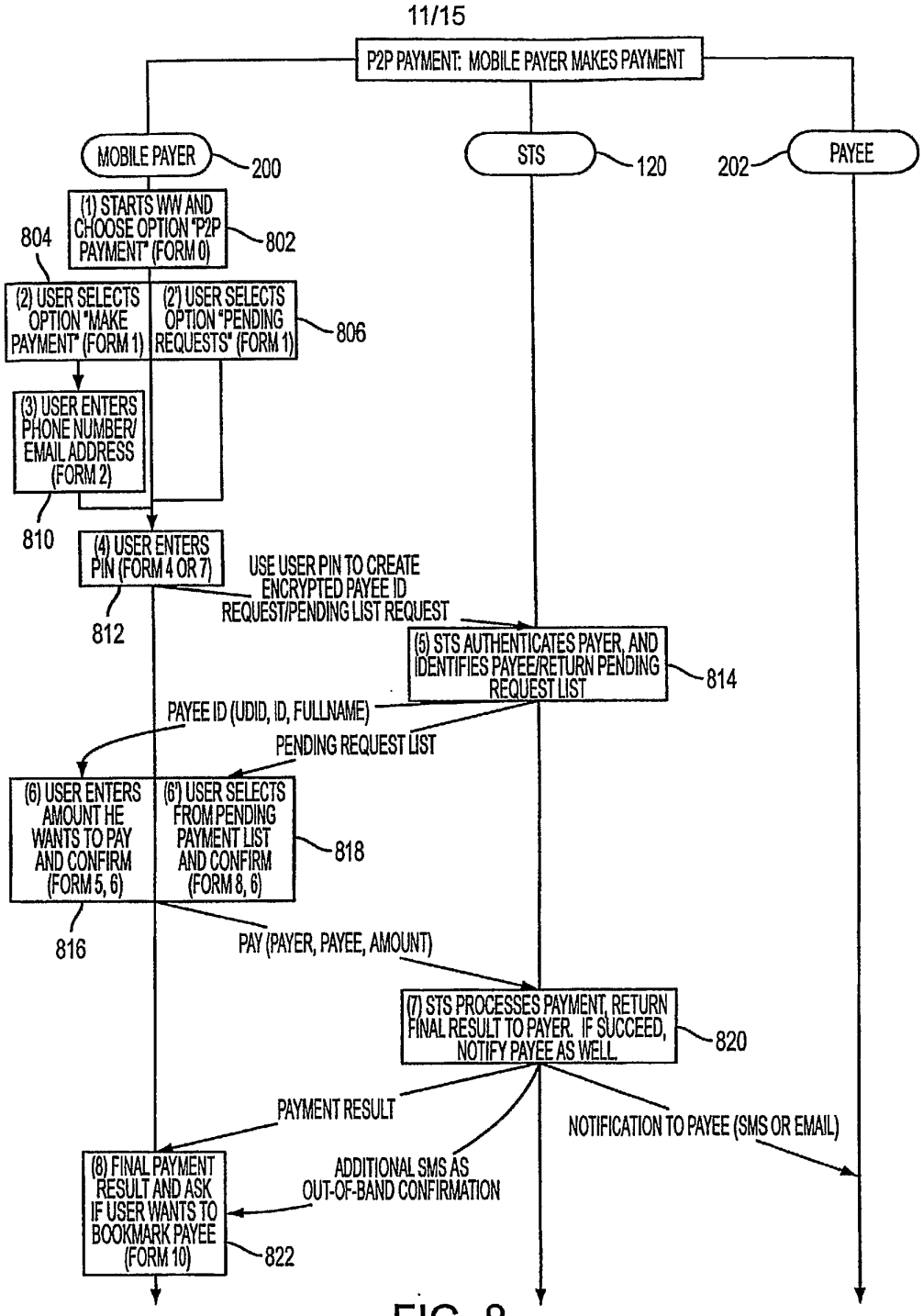

P2P PAYMENT: MOBILE PAYER MAKES PAYMENT
MOBILE PAYER
200
STS
120
202
PAYEE
(1) STARTS WW AND CHOOSE OPTION "P2P PAYMENT" (FORM 0)
802
804
(2) USER SELECTS OPTION "MAKE PAYMENT" (FORM 1)
(2') USER SELECTS OPTION "PENDING REQUESTS" (FORM 1)
806
(3) USER ENTERS PHONE NUMBER/ EMAIL ADDRESS (FORM 2)
810
(4) 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

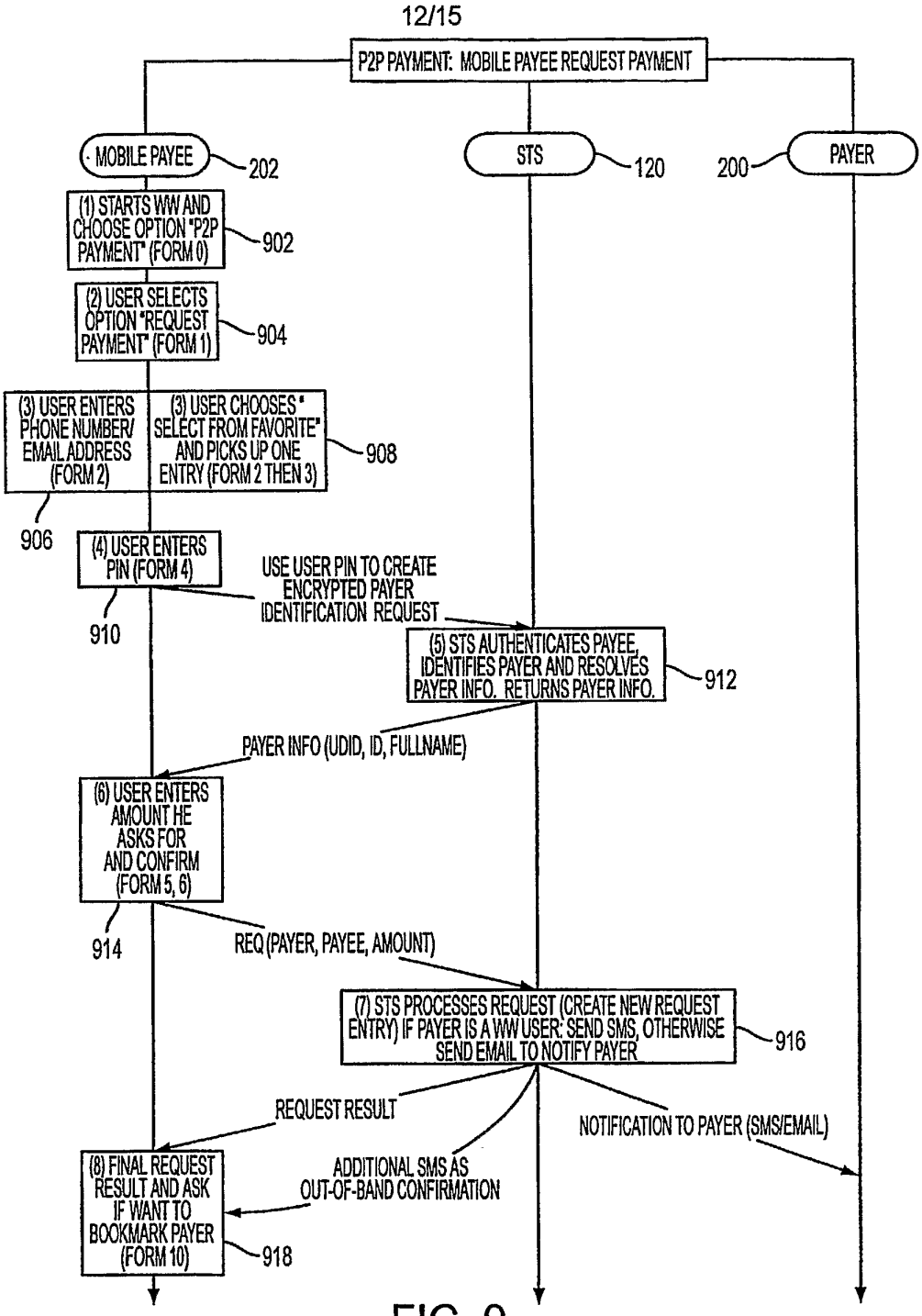

P2P PAYMENT: MOBILE PAYEE REQUEST PAYMENT
MOBILE PAYEE
202
STS
120
200
PAYER
(1) STARTS WW AND CHOOSE OPTION "P2P PAYMENT" (FORM 0)
902
(2) USER SELECTS OPTION "REQUEST PAYMENT" (FORM 1)
904
(3) USER ENTERS PHONE NUMBER/ EMAIL ADDRESS (FORM 2)
(3) USER CHOOSES "SELECT FROM FAVORITE" AND PICKS UP ONE 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

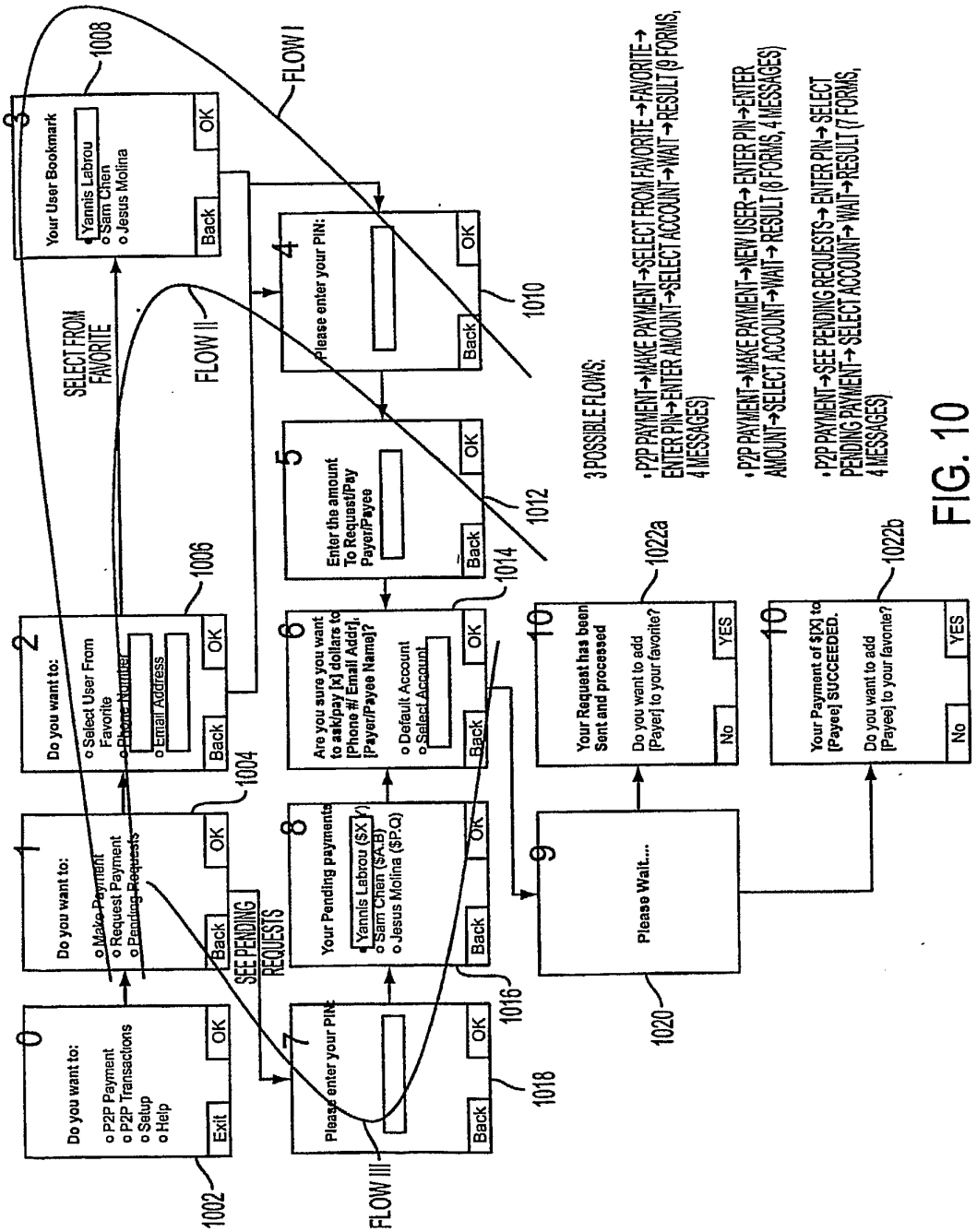

0
Do you want to:
o P2P Payment
o P2P Transactions
o Setup
o Help
Exit
OK
1002
1
Do you want to:
o Make Payment
o Request Payment
o Pending Requests
Back
OK
1004
2
Do you want to:
o Select User From Favorite
o Phone Number
o Email Address
Back
OK
1006
3
Your User Bookmark
Yannis Labrou
Sam Chen
Jesus 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 ($X.1)
Sam Chen ($X.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
SELECT FROM FAVORITE
SEE PENDING REQUESTS
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

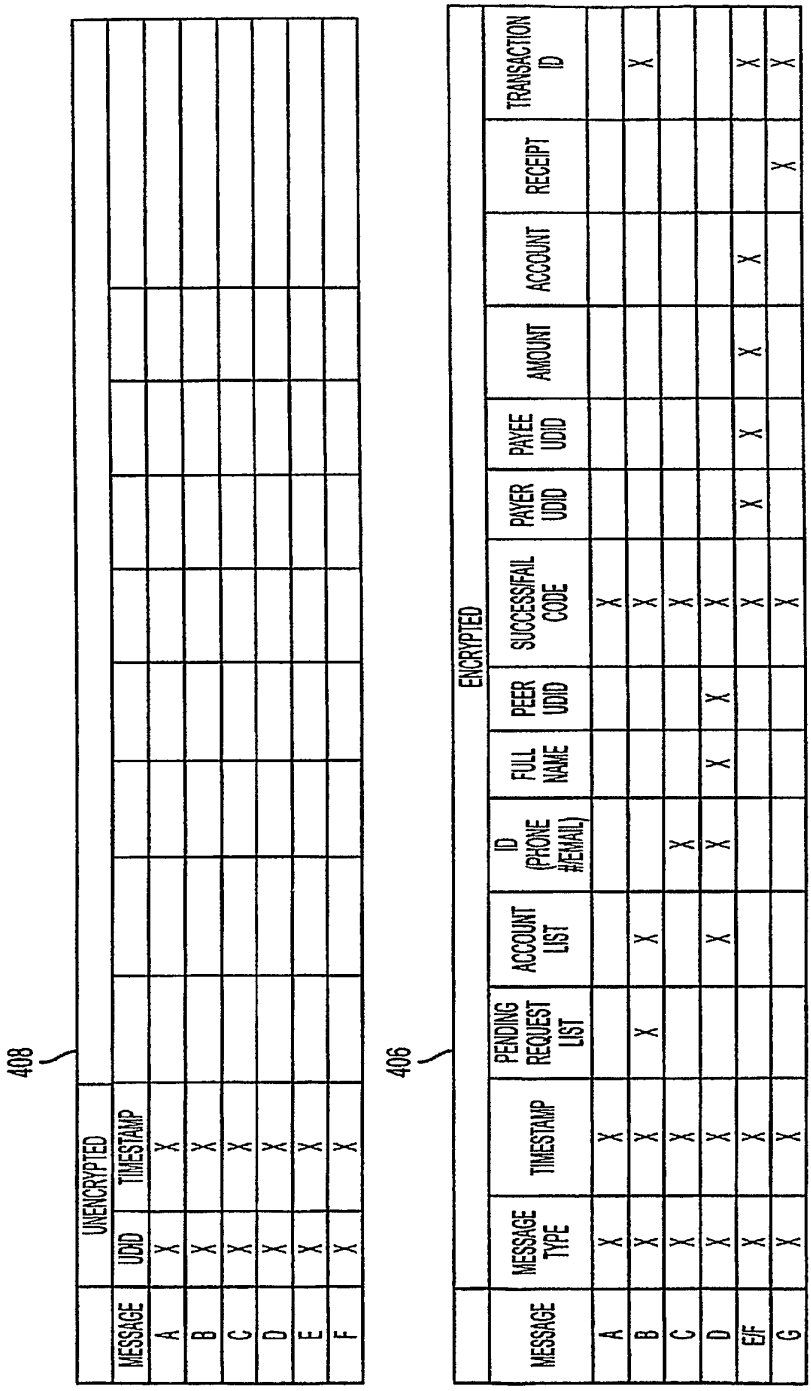

408
UNENCRYPTED
MESSAGE
UDID
TIMESTAMP
A X X
B X X
C X X
D X X
E X X
F X X
406
ENCRYPTED
MESSAGE
MESSAGE TYPE
TIMESTAMP
PENDING REQUEST LIST
ACCOUNT LIST
ID (PHONE #/EMAIL)
FULL NAME
PEER UDID
SUCCESS/FAIL CODE
PAYER UDID
PAYEE UDID
AMOUNT
ACCOUNT
RECEIPT
TRANSACTION ID
A X X X X X
B X X X X X X X
C X X X X X
D X 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

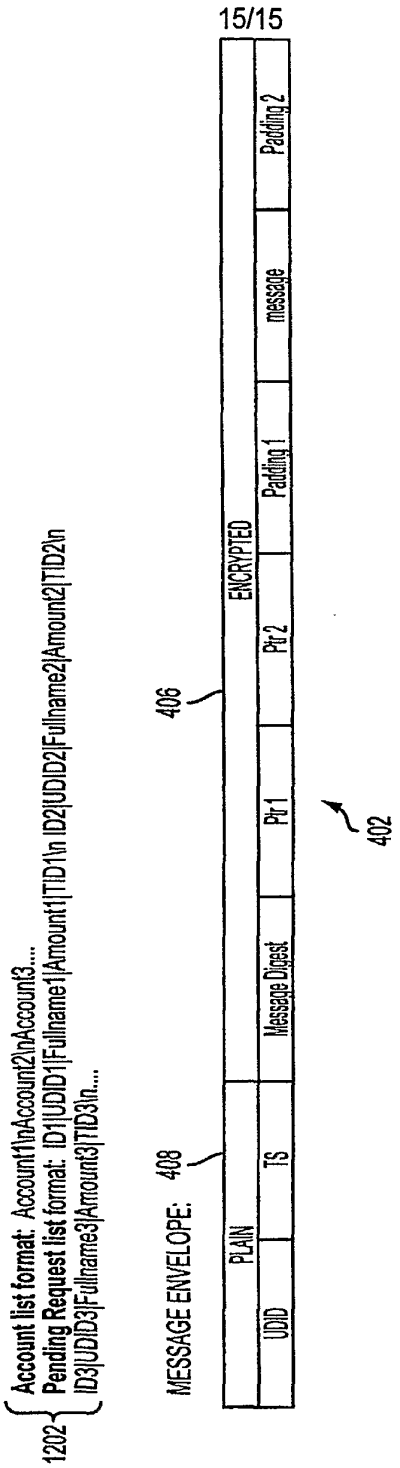

Account list format: Account1\nAccount2\nAccount3....
Pending Request list format: ID1|UDID1|Fullname1|Amount1|TID1\n ID2|UDID2|Fullname2|Amount2|TID2\n ID3|UDID3|Fullname3|Amount3|TID3\n....
1202
MESSAGE ENVELOPE:
408
406
402
PLAIN
ENCRYPTED
UDID
TS
Message Digest
Ptr 1
Ptr 2
Padding 1
message
Padding 2

FIG. 12

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086593 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IN2005/000038

(22) International Filing Date: 4 February 2005 (04.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
165/DEL/2004 5 February 2004 (05.02.2004) IN

(71) Applicant *(for all designated States except US)*: **A LITTLE WORLD PRIVATE LIMITED** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GUPTA, Anurag** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN). **PANDA, Lokanath** [IN/IN]; Flat No. : 103, Srinivasa Residency, 7th Cross, N. R. Colony, Bangalore 560 017 (IN).

(74) Agent: **VAIDYANATHAN, Alamelu**; 451, 2nd Cross, 3rd Block, 3rd Stage, Basaveshwaranagar, Bangalore 560 079 (IN).

(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, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

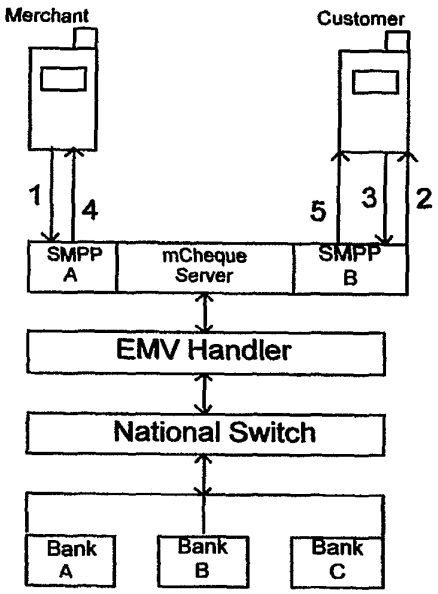
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, 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).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i)) 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,*

[Continued on next page]

(54) Title: INTER-OPERABLE, MULTI-OPERATOR, MULTI-BANK, MULTI-MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR



(57) Abstract: This invention relates to an inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

WO 2005/086593 A2

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, SM, 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, NA, 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, IS, IT, LT, 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 all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

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.

AN INTER-OPERABLE MULTI-OPERATOR, MULTI-BANK, MULTI-MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR.

This invention relates to an Inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone, a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

Introduction:

The existing financial transaction systems involve use of physical currency, debit and credit cards based on Magnetic Stripe technology. The Magnetic Stripe debit/credit card based transactions are inherently prone to security violations given to the fact that Magnetic Stripes can be easily read and duplicated. Also, there are disadvantages in terms of physical damage to the Magnetic Stripe after some swipes on a physical merchant terminal. The existing smartcard based transaction systems are secure, but mandate use of an expensive Point-of-Sale Terminal to carry out a financial transaction, be it a stored value transaction or an online/offline debit/credit transaction.

The secure and more reliable alternative lies in use of a mobile phone, which offers computational capabilities and guarantees security with cryptographic support in the phone/SIM operating system.

Europay Mastercard Visa (EMV) and Common Electronic Purse Scheme (CEPS) standards provide means for development of interoperabe payment scheme. In this context A.Little.World is implementing a new interoperable payment brand in India and abroad known as mCheque. mCheque platform provides a secure all-purpose debit/credit payment system on mobile phones.

APPL-1002
APPLE INC. / Page 1054 of 1892

The proposed solution enables the consumer (hereby referred to as 'payer' or 'customer') to carry out financial transactions from his/her Mobile Phone with debit/credit cards configured on the Mobile Phone and helps the merchant (hereby referred to as 'payee' or 'merchant') to use a hosted Virtual Terminal service, while the mobile phone of the merchant is used as the payment terminal. However the payer can use the debit/credit card(s) configured on the Mobile Phone to engage in a payment transaction with the payee application on the regular Point-of-Sale Terminal, Vending Machine, Internet or ATM.

Large-scale use of mobile-to-mobile payment between customers and merchants - using any mobile phone as an EMV debit/credit payment instrument issued by a Bank, to pay any merchant who has another mobile phone. No additional terminal infrastructure apart from mobile phone is required by Bank or by merchants. No compromises made on transaction security.

Funds flow will be handled entirely through the banks, using proven EMV security with the added layer of mobile network security for secure communications. The EMV handler will provide an effective intermediary solution to the Bank without need for the Bank having to upgrade its back-end infrastructure to EMV.

Public Key Infrastructure (PKI) will be used for non-repudiation in specific application areas. Mobile Phones will have the capability of a universally usable digital ID (to be issued as an X.509 certificate by a Certification Authority) for digitally signing transactions for non-repudiation. RSA is the preferred standard for security implementation for PKI applications of mCheque.

The application download and personalization of the mobile phone can be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end as a Virtual Terminal, with the phone used for confirmation of the transaction (transaction receipt).

The ready availability of communications network; the display screen; and the large memory on the phone to store and view transaction records helps enhance the Bank's product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

PRIOR ART:

There are known instances of various forms of payment mechanisms using mobile devices, such as Singapore Patent Publication No. 86428 using a payment center backend without use of real debit/credit card and involving a bank in the transaction.

US Patent No. 6,612,488 describes a method of payment using credit cards using a portable communication terminal such as a cellular phone. However, this method does not avoid the use of the credit card or debit card. The portable communication terminal is used to only identify the purchaser to avoid fraudulent use of the cards.

US Patent No. 6, 678, 664 issued to CheckFree Corporation suggests cashless transactions, e.g. purchases of goods and services without making cash payments at the time of purchase, by transmitting, preferably from a point of purchase, information identifying the purchaser of a product without identifying a payment account for the purchaser, the point of purchase being, for example, a register within a retail store or a server at an internet site.

Though the aforesaid US patent suggests the use of personal identification information such as purchaser's name, address and drivers license or passport number or any other identification code, this process of identification is little cumbersome and yet requires some document to be carried by the purchaser. Further, the transaction cannot be completed by using a wireless communication device and also it does not offer a virtual terminal to the seller. In other words, the seller is required to have a terminal, a scanner or other similar means to transmit the personal identification details to the bank or to the payment operator.

Objects of The Invention:

- The primary object of the present invention is to provide an inter-operable, multi-operator, multi-bank, multi-merchant, mobile payment method and system.

- In the proposed payment method/system, a regular mobile phone is used as a bank-account linked debit/credit payment instrument to pay any merchant with a regular mobile phone, without customisation of phone hardware. The merchant does not need a regular payment terminal. However, the merchant terminal can be a regular Point-of-Sale terminal, vending machine, Internet or ATM.

- Genuine 'card present' transactions using debit/credit cards configured on the mobile phone.

- EMV Handler solution enabling banks to participate in the secure debit/credit card based transactions without having to migrate to EMV.

The following is the scope of the mCheque payment method/system:

Use a regular mobile phone as an EMV-based payment instrument linked to a debit or credit account in a Bank, to pay any merchant who has a mobile phone or an on-line EMV capable terminal. The merchant does not need a regular payment terminal. EMV security is fully implemented for this product.

The ready availability of a communications network; the display screen on the mobile; and the large memory on the phone to store and view transaction records helps enhance the product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time. Multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

In case of availability of a Subscriber Identification Chip module on the phone (SIM for GSM and R-UIM for CDMA), the application is developed without need to customize either the phone hardware or software. The only change is made to the SIM/R-UIM software through the use of the SIM Application Toolkit or a script using existing SIM/R-UIM browsing environment. In case of phones without having a Subscriber Identification Chip module, the application is developed on the phone. As a result, nearly the entire base of mobile phones can be used as cards and terminals without extra investment required in cards or terminals. The payment application for debit/credit card on payer's mobile phone and the merchant terminal on payee's mobile phone use security mechanisms prescribed by EMV.

The application download and personalization of the mobile phone will be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end, with the phone or a connected PoS terminal being used for confirmation of the transaction (transaction receipt).

The EMV handler solution will be used to provide an effective intermediary solution to banks that have not yet upgraded their back-end infrastructure to EMV. This applies both to the debit/credit card issuance, transaction authorization and merchant acquiring systems of the bank.

The transactions will be cleared and settled domestically through the inter-bank switch for domestic transactions or an international settlement agency for cross-border transactions. Security Key management will be provided by the scheme operator or the domestic banking regulator for both Symmetric Keys based on 3-DES or AES and Asymmetric Keys based on RSA.

Multiple mobile operators and multiple issuer and acquiring banks can be part of the system. Funds flow is handled entirely through the banking system, using proven EMV security with the added layer of GSM/CDMA security for secure communications.

The mCheque Platform in its true sense of 'Interoperability' is intended to support existing systems and technologies used by mobile operators, mobile phones, transaction systems and banks.

The following are the unique features of the present invention:

a. Use of mobile phone as a debit/credit card.
b. Use of mobile phone as a merchant terminal.
c. Use of mobile phone to have multiple debit/credit cards
d. Use of mobile phone to store Track-2 data of a debit/credit card.
e. Responsibility of Authentication of mobile debit/credit card transaction lies with the bank and not with mobile operator.
f. Provisioning of debit/credit card on mobile phone without a contact interface using OTA interface.
g. Provisioning of digital certificate on mobile phone without a contact interface using OTA interface.
h. EMV Handler: Authorization of transaction security on behalf of banks. Ability to handle EMV Transactions in a multibank interoperable environment without enforcing the banks to change their existing infrastructure.

i. Providing printed payment receipt using a mobile phone, wherever possible without making any change on the mobile phone hardware using an external receipt printer.

j. Payment over Internet using debit/credit card on mobile phone.

k. ATM cash-withdrawal using bank card on mobile phone.

l. Person-to-person transfer of payment or funds transfer using mobile phone both domestic and international.

m. Use of Public Key Infrastructure on mobile phones for transactions requiring non-repudiation.

n. Maintaining and managing loyalty pools and coupons on mobile phone.

This invention thus provides a multi-bank interoperable payment system using mobile phone as debit/credit card which comprises the steps of:

(i) establishing connectivity with multiple mobile operators, issuing banks and acquiring banks participating in the "interoperable mCheque system" and inter-bank clearing & settlement systems, both domestic and international, via the mCheque back-end system/issuance system;

(ii) establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator. A third party Certification Authority can provide certificates to establish mutual authentication and trust between different systems.

(iii) providing transaction security which is dependent on the bank's security domain defined on the mobile phone. The mobile network is used as a transport and the system does not necessarily depend on the security provided by the mobile network to guarantee transaction security. However, the security provided by the mobile network is treated as a complementary measure.

(iv) Application Provisioning Step-1: loading of payment application containing the basic menus, transaction logic, application security keys

and application configuration data; on the target mobile phone of payer/payee using the over-the-air system of the mobile operator;

(v) Application Provisioning Step-2: loading of a conventional Track-2 data provided by the participating bank with EMV security keys and risk management parameters on the target mobile phone of payer using the over-the-air system of the mobile operator; and

(vi) Application Provisioning Step-3 (optional): loading of a digital certificate on the target mobile phone of payer/payee using the over-the-air system of the mobile operator requiring non-repudiation; and

(vii) establishing a link between the PIN number allotted to the customer and a common mCheque PIN.

The system takes care of post-issuance activities including blocking/unblocking of debit/credit card, creation/deletion of debit/credit cards, update loyalty pool, loyalty redemption, offering of loyalty coupons, blocking/unblocking/resetting of PIN, key version control, application version control, restoration of debit/credit accounts and loyalty details for a lost/stolen mobile phone.

This invention will now be described with reference to the accompanying drawings, wherein:

Fig. 1 illustrates the mCheque transaction flow;

Fig. 2 illustrates the mCheque transaction system;

Fig. 3 illustrates the mCheque Card Issuance/Merchant Configuration System; and

Fig. 4 illustrates the mCheque Digital Certificate System.

The use of mobile phone as a debit or credit card involves the following five steps, which is illustrated in Fig. 1.

1. Payee Mobile sends a message through mobile network to mCheque back-end with Payer Mobile Number, Transaction Amount and a Random Number.

APPL-1002
APPLE INC. / Page 1061 of 1892

2. mCheque back-end sends a message through mobile network to Payer Mobile with Random Number, Request for Payment and Merchant Details.
3. Payer Mobile sends a message to mCheque back-end through mobile network with EMV Cryptogram.
4. mCheque back-end through mobile network sends a message to Payee Mobile with Transaction Receipt.
5. mCheque back-end through mobile network sends a message to Payer Mobile with Transaction Receipt.

Message-1: Payment Request Message Originating from Merchant

1. Merchant enters the Amount of Transaction, Customer's ID (generally customer's mobile number or a proxy number similar to the mobile number assigned by mCheque) and Merchant PIN using mCheque menus.
2. mCheque Application on Merchant device generates a Random Number (to be used as the seed for the Application Request Cryptogram to be generated on Customer's Mobile Phone for EMV transaction) and signs the transaction data.
3. The Merchant Mobile Phone initiates a session with the mCheque Server and sends the signed data.

Message-2: Confirmation Request Message Terminating on Customer Mobile

1. The signed message from Merchant reaches mCheque Virtual Terminal Application Server (VTAS), which verifies the signature and adds EMV specific terminal risk management parameters and Merchant's Name to the original transaction attributes provided by the merchant.
2. mCheque VTAS initiates a session with Customer Mobile Phone.

APPL-1002
APPLE INC. / Page 1062 of 1892

Message-3: Confirmation Response Message Originating from Customer Mobile

1. Customer Mobile Phone receives the message-2 and displays a confirmation message consisting of Merchant Name, Transaction Amount and Merchant Id. Up on confirmation by the customer, a PIN entry is requested.
2. Up on successful PIN entry, the Customer Mobile Phone generates an Application Request Cryptogram (ARQC) as per EMV specifications using the Card Risk Management Parameters, Random Number, Card Master Key (of the key index assigned for the application in the card security domain).
3. Customer Mobile Phone sends the transaction data with the ARQC to mCheque VTAS.

Message-4: Transaction Receipt Message Terminating on Merchant

1. mCheque VTAS sends the transaction online for authorization of funds
2. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Merchant.
3. After confirmation of Receipt delivery, mCheque VTAS issues a Transaction Certificate to the online authorization system of Issuing Bank (denoting completion of transaction).

Message-5: Transaction Receipt Message Terminating on Customer Mobile Phone

1. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Customer Mobile Phone.

To achieve the above, the present invention provides a transaction system (refer Fig. 2 and 3) which comprises of an unique mCheque virtual terminal capable of handling communications from mobile phones of the payer and payee and also ensure security of the transaction, said server having means for customer database and merchant data base, means for providing hardware security, means for storing the digital certificates and application software for life cycle management of payer/payee application.

The process of obtaining a Digital certificate is illustrated in Fig. 4. The mobile phone of the user or purchaser through the personalization system of mCheque issuance system will send in the necessary request to the certification authority and after processing the request, the certification authority will forward the required certificate through to the personalization system of mCheque issuance system back to the mobile phone of the payer/payee.

The following middleware and application systems constitute the mCheque technology platform:

Backend and Middleware Modules:

- **Virtual Terminal Application Server (VTAS):**

VTAS is a secure cluster of virtual EMV terminals, security systems, loyalty systems, bank/operator interfaces running on a High-Availability platform. All mCheque messages originating from the merchant as well as the customer mobile are routed to the VTAS Server. VTAS spawns one instance of Virtual Terminal Application per Merchant Terminal registered in the mCheque system.

- **USAT Interpreter:**

Application Gateway to interpret and perform application codec (encoding/decoding) functions for data flow between VTAS and Mobile phone.

APPL-1002
APPLE INC. / Page 1064 of 1892

- **EMV Handler:**

The mCheque EMV Handler performs secure authorization of EMV Application Request Cryptogram (ARQC) generated by the chip card EMV application (debit/credit card) on the customer's mobile phone and generates an EMV Application Response Cryptogram (ARPC). The EMV Handler filters EMV specific data from the financial transaction message and the transaction is sent to the Issuing Bank for funds authorization as if it were a regular magnetic stripe transaction authorization request. The EMV Handler therefore provides an effective intermediary Issuing and Acquiring solution for Banks to work with chip cards based on EMV security without having to upgrade their back-end systems to EMV. In case an Issuing Bank is capable of handing EMV transactions directly, the transactions will be directly passed through for authorization by the Bank's EMV Switch. The EMV handler system uses a Hardware Security Module compliant to FIPS-140-2 and PKCS#11 standards to carry out all security operations.

- **Remote Personalization System:**

The mCheque Remote Personalization System provides secure personalization of EMV based secure Debit/Credit cards, Loyalty Pools, Coupons on Mobile phone of mobile phones Over-the-Air (OTA). The Remote Personalization System also uses the OTA bridge for personalization as well as application updates (such as update of EMV risk parameters). Multiple accounts can be handled on a single Mobile phone by this system. The remote personalization system uses a Hardware Security Module to carry out security operations.

- **OTA Bridge:**

Application system providing a secure transport of personalization and transaction data between the mCheque Application Backend (VTAS) and the Network Gateway of mobile operators (USSD Center/SMS Center) for all Over-the-Air application operations on payer/payee mobile phones. The OTA Bridge also takes care of security requirements of the mobile operator.

- **USSD-IP Gateway:**

Network gateway providing exchange of Unstructured Supplementary Service Data (USSD) messages between the Mobile Station and the IP-based backend of mCheque Payment Platform. The mCheque USSD-IP Gateway is co-located with the Master Switching Centre (MSC) of the Mobile Operator through an SS7 (Signaling System 7) link.

- **Transaction Switch:**

Host system to switch financial transactions between Switches of participating banks in ISO 8583/XML formats. This system is also used to log the clearing data provided as input to the central Clearing and Settlement Host.

- **Clearing and Settlements Host:**

This system is used process the data that passes through the Transaction Switch to create logs for daily reconciliation to be performed either through a Clearing and Settlements Bank or an automated system. The Clearing and Settlement Institution will be given summaries for net settlements between participating Banks and each participating bank will be given detailed logs of all transactions performed by its customers.

- **MIS and Reporting Tools:**

Management Information System of mCheque Payment Platform includes reporting, logging and audit trail of transactional and operational data for all participating entities in the system, including merchants, customers, issuing banks, acquiring banks, mobile operators and personalization system.

- **ATM Module:**

An application specification will be provided for enhancement of the ATM customer screen to be able to accept ATM cash withdrawal transactions using mCheque. This requires collaboration with ATM vendors and the respective Banks.

Applications

- Over-the-counter debit/credit payment for small, large and very large amounts. PIN based debit/credit using secure EMV based technology on any mobile phone.
- More versatile than debit/credit cards.
- Display screen, PIN pad and storage add tremendously to usability, convenience and control.
- Multiple cards/accounts can be issued by multiple banks on one mobile.
- Only one PIN to remember - common PIN for all cards/accounts.
- Transaction amount limits and daily limits can be managed on mobile phone.
- Common rewards points pool across all cards/accounts.
- Small value transactions feasible in both credit and debit mode.
- Transaction details stored on mobile phone.
- Balance enquiry.
- Full audit and traceability.
- Unique new method to receive payments: eliminates need of cheque-book.
- PKI based non-repudiable digital-ID and signatures on mobile phone. Ideal for all kind of Government payments and transactions.
- Secure and convenient payment for Internet purchases (unique new method with highest level of security and convenience).
- Instant, anywhere, anytime payment of utility bills; insurance premiums; mobile phone bills; pre-paid top-ups.
- Payment to vending machines (snacks, beverages, etc.).
- Cash withdrawal at ATM machines with subscription based access to large number of ATMs in arrangement with banks.
- Loyalty points-pool-on-mobile phone for accumulating rewards from different merchants. Instant over-the-counter redemption.

The applications are developed without need to customize either the mobile phone hardware. As a result, the entire base of mobile phones available can be used as debit/credit cards and payment terminals without any significant extra investment.

CLAIMS:

1. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment method using mobile phone as debit/credit card comprising the steps of:
   a. establishing connectivity with each mobile operator, issuing bank and acquiring bank participating in the "interoperable mCheque system" and in any inter-bank clearing & settlement systems, via the mCheque back-end system/issuance system;
   b. establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. loading of payment application containing the basic menus, transaction logic, application security elements and application configuration data;
   e. loading of at least one conventional Track-2 data provided by the participating bank of the payer, EMV security elements and risk management parameters on the target mobile phone using the over-the-air system of the mobile operator; and
   f. optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and
   g. establishing a link between the PIN number allotted to the customer and the common mCheque PIN.

2. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of payment application is carried out using application provisioning step-1.

3. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of Track-2 data provided by the participating bank is carried out using application provisioning step-2.

4. An inter-operable mobile payment method as claimed in claim 1, wherein the optional loading of the digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation is carried out using application provisioning step-3.

5. An inter-operable mobile payment method as claimed in claim 1, wherein multiple debit/credit card Track-2 data are loaded on the mobile phone.

6. An inter-operable mobile payment method as claimed in claim 1, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

7. An inter-operable mobile payment method as claimed in claim 1, including software for maintaining and managing loyalty pools and coupons on mobile phone.

8. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment system using mobile phone as debit/credit card comprising of;
   a. mCheque back-end system/issuance system comprising means for establishing connectivity with each mobile operator and issuing bank participating in the "interoperable mCheque system" and in any inter-bank clearing and settlement systems;
   b. Means for establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. Means for providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. Application provisioning software I to enable loading of payment application containing the basic menus, transaction logic and application configuration data;
   e. Application provisioning software II to enable loading of at least one conventional Track-2 data provided by the participating bank on the target mobile phone using the over-the-air system of the mobile operator;

APPL-1002
APPLE INC. / Page 1069 of 1892

f. Application provisioning software III for optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and

g. Means for establishing a link between the PIN number allotted to the payer and the common mCheque PIN.

9. An inter-operable mobile payment system as claimed in claim 7, wherein multiple debit/credit Card Track-2 data are loaded in the mobile phone.

10. An inter-operable mobile payment system as claimed in claim 7, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

11. An inter-operable mobile payment system as claimed in claim 7, including software for maintaining and managing loyalty pools and coupons on mobile phone.

12. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of user is used as debit/credit card.

13. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of the merchant is used as merchant terminal.

APPL-1002
APPLE INC. / Page 1070 of 1892

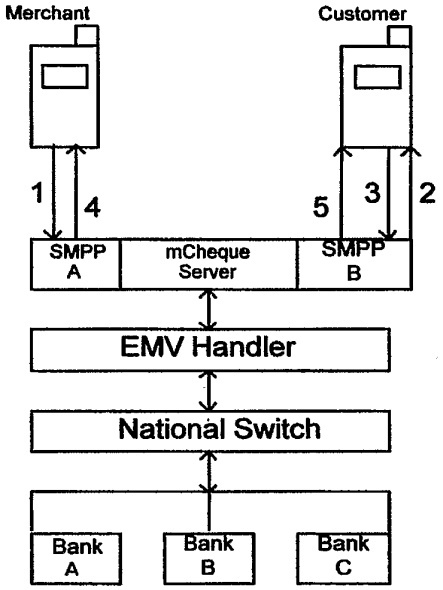

Merchant
Customer
1
4
5
3
2
SMPP A
mCheque Server
SMPP B
EMV Handler
National Switch
Bank A
Bank B
Bank C

Fig. 1.

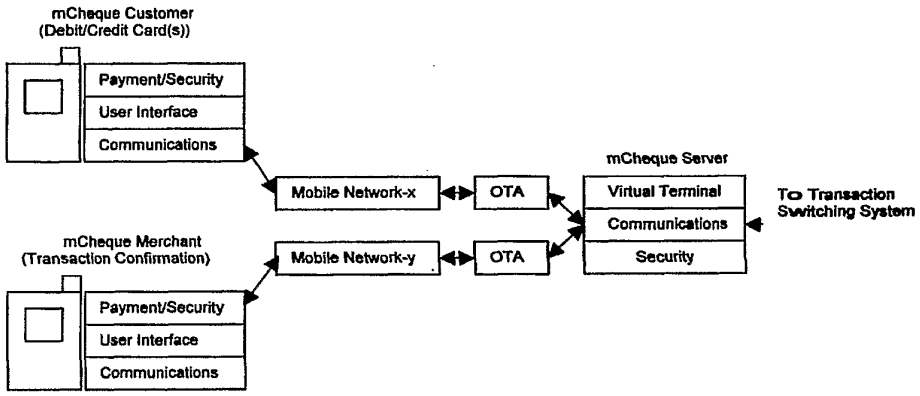

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
Mobile Network-x
OTA
mCheque Server
Virtual Terminal
Communications
Security
To Transaction
Switching System
mCheque Merchant
(Transaction Confirmation)
Mobile Network-y
OTA
Payment/Security
User Interface
Communications

Fig. 2

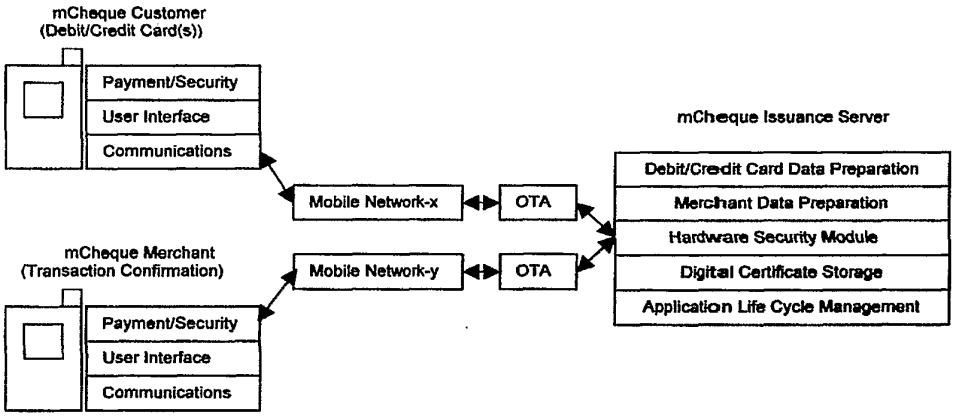

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
mCheque Merchant
(Transaction Confirmation)
Payment/Security
User Interface
Communications
Mobile Network-x
Mobile Network-y
OTA
OTA
mCheque Issuance Server
Debit/Credit Card Data Preparation
Merchant Data Preparation
Hardware Security Module
Digital Certificate Storage
Application Life Cycle Management

Fig. 3

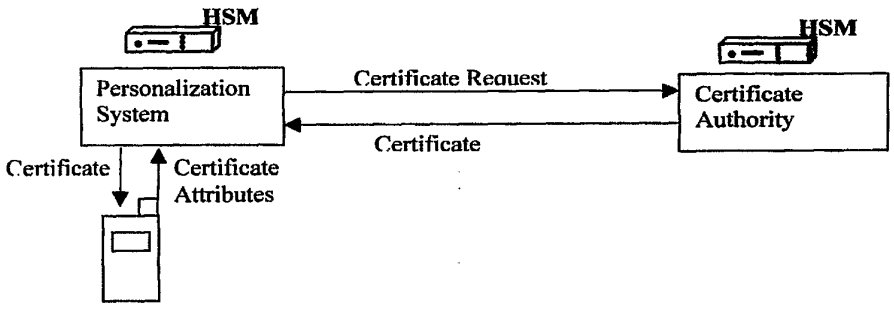

HSM
HSM
Personalization System
Certificate Request
Certificate Authority
Certificate
Certificate
Certificate Attributes

Fig. 4.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2007 (21.12.2007)

PCT

(10) International Publication Number
WO 2007/145500 A1

(51) International Patent Classification:
G07F 19/00 (2006.01) *G06Q 10/00* (2006.01)
G06Q 20/00 (2006.01) *H04M 15/00* (2006.01)
H04M 17/00 (2006.01)

(21) International Application Number:
PCT/MY2007/000038

(22) International Filing Date: 11 June 2007 (11.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20062712 12 June 2006 (12.06.2006) MY

(71) Applicant *(for all designated States except US)*: **MOBILE MONEY INTERNATIONAL SDN BHD** [MY/MY]; Lot 23-24, 2nd Floor, I.O.I. Business Park, 47100 Puchong, Selangor (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LOH, Jin, Feei, Jeffrey** [MY/MY]; 55 Jalan BU 10/7, Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan (MY). **LEE, Eng, Sia** [MY/MY]; 18 Halaman York, Georgetown, 10450 Penang (MY).

(74) Agent: **CHEW, Kherk, Ying**; Wong & Partners, Level 41 - Suite A, Menara Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur (MY).

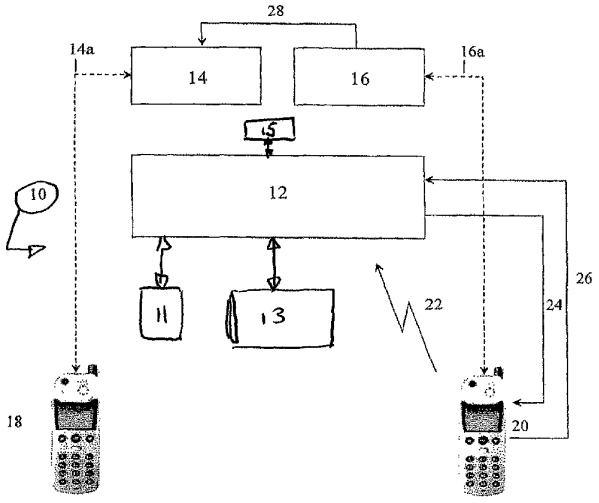
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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, LV, MC, MT, 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).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: TRANSACTION SERVER



(57) Abstract: A transaction server is disclosed that has a receiver module configured to receive an instruction message from a first mobile communications device for a transaction from a first account to a second account. The transaction server also has a transmission modul configured to send a response message to the first mobile communications device a request for a validation instruction for the transaction, the response message being in response to the receipt of the instruction message. The server is configured to record receipt of the validation instruction. The server is also configured to record receipt of the validation instruction. In response to the validation instruction, the server validates and effects the transaction. A corresponding method is also disclosed.

WO 2007/145500 A1

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.

TRANSACTION SERVER

Technical Field

The invention relates to a transaction server for effecting transactions from a user account. More particularly, the invention relates to validating transactions from the user account.

Background

Systems for implementing mobile phone based payments where, essentially, a mobile telephone acts as an electronic wallet (e-wallet) are known. In such systems, a monetary value is held in an e-wallet for each user, and the details of each e-wallet are stored centrally in a server database.

With a mobile telephone, transactions may be conveniently and commonly effected using a messaging service such as SMS. For example, to send $20 from a first e-wallet identified or associated with a first mobile phone +60122070239 to a second e-wallet identified with a second mobile phone +60164452228, the following SMS is sent:

```
PAY 0164452228 20 753535
```

As can be seen, the text string of the message comprises several fields: "0164452228" is the recipient mobile telephone's number; "20" is the transfer amount (e.g. $20); and 753535 is a six-digit PIN associated with the user and/or the e-wallet +60122070239. The server receives this SMS through a telecommunication link to an SMS centre or portal.

Such a system is attractive because it facilitates money movement. It means practically anyone, anytime, anywhere can be paid. For example, to pay a friend several miles away all a user need do is to use their mobile telephone to send a simple SMS to the SMS portal to effect payment from the e-wallet or account.

Unfortunately, such a system has several drawbacks which, if not properly addressed, can adversely affect its implementation and security.

Messaging services such as SMS as a means of communication are never 100% reliable. A sender of an SMS never knows for certain if the message will be delivered or when. Sometimes an SMS is delivered to the same recipient multiple times. These failings of SMS are particularly problematic for e-wallet transactions. For example, a user may be at a shop and use their mobile telephone to send an SMS to the server's SMS portal requesting payment for goods to the shop owner's account. However, it is possible that the mobile telephone may not receive acknowledgement from the server that the payment request has been either received, or that payment has been initiated. Such situations can arise during a period of peak use of the SMS system or, simply, the SMS is "dropped" by the messaging service. In such situations, the user is presented with a quandary. What should the user do? Should the user just leave? Should the user send another payment request? The server might receive the user's first SMS and effect the transaction the moment after a second instruction SMS is sent, or the user gives up and leaves the shop. Alternatively, the server might receive several copies of the single SMS and the server effects multiple payments to the shop owner for a single transaction. The user is unlikely to be able to receive any real help from the help centre for the server as the call centre may advise the user that the SMS has not arrived yet and that no transaction has been effected so far. Conceivably, the SMS could arrive at the server the very moment the user terminates the telephone call with the call centre.

Another problem is human error. Inevitably, users will key in a wrong recipient's mobile number or incorrect transaction amount in the SMS. The user may call the call centre to request a reversal. In cases like these, security for the recipient could be compromised – e.g. the recipient is a shop owner who has provided goods or services in good faith to an e-wallet user. Should the call centre do the reversal? The user may have just bought something from the shop owner and requested a reversal the moment after the goods were collected or the user has left the shop.

Security is another problem. It is a well-known fact that SMS can be spoofed quite easily. If a fraudster somehow manages to obtain a person's PIN, the fraudster can spoof an SMS message to the server to instruct a transaction quite easily.

Summary

The invention is defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

If the transaction instruction (e.g. SMS from the user to the server) is delayed or not delivered, the user knows very well no transaction has been effected from his account (e-wallet) as the user is neither requested to provide the validation instruction and, therefore, it is not possible for the user to provide the validation instruction. If the user receives a request for the validation instruction from the server at a later time seeking validation for the transaction, the user then has the option to proceed with the validation instruction for the transaction or to decline to send the validation instruction. In the event the server receives multiple copies of the transaction instruction (e.g. SMS), the server may be configured also to send multiple requests for validation in the form of SMS messages to the user seeking confirmation and the user can choose how many of these requests for a validation instruction he/she can reply to, if any. In embodiments of the invention, each request for validation provides different instructions for effecting the validation instruction (e.g. different telephone numbers are provided for the user to call to validate the transaction). The user may then selectively choose whether and how many times the recipient in the transaction is to be paid. Optionally, additional information such as the account (e-wallet) balance and details of previous transactions are included in the request for the validation instruction.

Further, the likelihood of user error is now significantly reduced. In embodiments of the server, the server is configured to look up the recipient's name from a server database, and to transmit the requested recipient's details to the user with the request for the validation instruction to the user. Optionally, the transaction amount is also shown.

Yet further, the server provides enhanced security and fraudsters may find it more difficult to spoof the server. The server may selectively choose the means by which the user is to request validation of the transaction; e.g. in embodiments of the invention, a telephone number for the user to call or message to is randomly picked from hundreds of numbers; the user may be requested to enter a URL on the user's internet browser to request validation, or any of many other possible ways in which a communication can be effected. Thus, the fraudster will not know the number to call to confirm a transaction, or the URL to visit. This means the fraudster must intercept the request for validation of the transaction sent by the server and at the same time spoof a user ID.

Brief Description of the Drawings

Exemplary embodiments will now be described, by way of example only, and with reference to the accompanying drawings. In the drawings:

Fig. 1 is a block diagram illustrating implementation of an exemplary;

Fig. 2 is a flow diagram illustrating the process of the implementation of an exemplary embodiment;

Fig. 3 illustrates the process of an exemplary embodiment; and

Fig. 4 illustrates a schematic view of the basic structure of an e-wallet system.

Detailed Description of the Exemplary Embodiments

Implementation of a transaction with a transaction server is illustrated in Figure 1. The system 10 comprises a transaction server 12, a first e-wallet 14 representing/being associated with a first account, and a second e-wallet 16 representing/being associated with a second account. The first e-wallet 14 is associated with the mobile communication device 18 and in particular with the owner of mobile communications device 18. Association with the device 18 is represented by the dashed line 14A. Association of second e-wallet 16 with the second mobile communication device 20 is represented by the dashed line 16A. Mobile communications devices 18, 20 may be a mobile telephone, portable telephone, cellular telephone, PDA, a device such as a "Blackberry", or telecommunications-enabled portable computer such as a laptop computer, notebook computer, tablet computer, and so forth.

To effect a transaction, the second communication device 20 is used to send a message 22 via a messaging service – e.g. SMS, MMS or email – to a receiving module such as, for example, the SMS portal 13 of server 12. The intended transaction is for the transfer of a sum of money to the e-wallet 14 of the first user being the user of communication device 18. The message 22 takes the form of:

```
PAY 0164452228 20 753535
```

As discussed above, the first field is the instruction "PAY", second field in the transaction instruction is an identifier for the recipient account preferably being the telephone number of first communication device 18; third field "20" is the value of the transaction; and the fourth field 753535 is an authentication code for the transaction, for example, a PIN of the second communication device 20 or a specific authentication code for the transaction. This provides a first level of security for the transaction. Responsive to receiving the instruction 22 from the device 20, the server 12 first matches the authentication code of the fourth field with the stored authentication code (extracted from the server 12 by, for example, recognition of the telephone number of the communication device 20 and using a look-up table to find the authentication code) and a transmission module 11 of the server sends to the device 20 a request 24 for the transmission of a validation instruction for the transaction. In embodiments of the server 12, this request may also be sent via a messaging service. Should the second user at device 20 wish for the transaction to be processed, the device 20 is then used to send a validation instruction 26 to the receiving module 13 of server 12. The server 12 records receipt of the validation instruction 26 and, responsive to this, the server 12 validates the transaction. Embodiments of the server then effect the transaction 28 of (in this example) $20 from second e-wallet 16 to first e-wallet 14.

Embodiments of the server 12 allow for the communication device 20 to be used to make a telephone call to a communications module 15 of the server 12 (or another communications portal) to provide the validation instruction. The request for the transmission of a validation instruction may, in embodiments of the server 12, provide details of the telephone number at server 12 to be called.

Embodiments of the server 12 are configured only to allow receipt of reliable means of communication for the request for validation: e.g. a telephone call, a message sent through GPRS (General Packet Radio Services) or through a secure (e.g. encrypted) internet communication.

It will be appreciated that one or more of the communications portals 11, 13, 15 may be distinct from server 12, may be used to send and receive communications from the devices 18, 20. In such embodiments of the server 12, the server 12 is configured to initiate and control sending and receipt of these instructions, so that a transaction may be effected from an account/e-wallet 16.

It will be further appreciated that embodiments of the server 12 allow for the e-wallets 14, 16 to be integral with the server 12.

In embodiments of the server 12, the server 12 is configured to validate the transaction if receipt of the validation instruction is recorded by the server 12 within a pre-determined period from sending, to the communication device 20, the request 24 for the transmission by device 20 of a validation instruction. If the receipt of the validation instruction 26 is not recorded by the server 12 within that pre-determined time period, the transaction may be voided.

After the server 12 receives a transaction request 22 (say at 5:15pm 24th May) from the device 20, the server 12 forwards to the device 20 the following SMS message, seeking confirmation:

```
Please confirm $20 transfer to 0164452228 (Lee Eng
Sia) by calling 0320540301. This message expires
5:25pm 24/05.
```

Thus, the request for the validation instruction confirms the identifier for the recipient account for the transaction. By doing so, the risk of human error in instructing a transaction to a wrong account may be reduced.

In exemplary embodiments of the server 12, the server 12 invites a telephone call to be made from communications device 20 to a telephone number (0320540301 above) to provide the validation instruction 26. In exemplary embodiments, the server 12 employs a pool of several hundreds (or even thousands) of telephone numbers, and 0320540301 is selected from this pool. Exemplary embodiments of the server 12 are configured to select a different telephone number for different transactions. The selection may be random, or organised.

Exemplary embodiments of the server 12 allow for the telephone number to be called by device 20. It is not necessary for the telephone call to be connected; the server need only capture the caller identifier from the telephone call. Either the call may be disengaged the call after, say, two or three rings, or the server is configured to disengage the call once an ID of device 20 has been extracted from the call. From this, the ID may be determined, providing further enhanced security for the transaction. Thus, there is no requirement for incurring unnecessary cost in actually connecting the telephone call to provide the validation instruction.

Thus, in exemplary embodiments of the server 12, the transaction will only be effected by the server 12 if the call 26 from the second mobile communications device 20 is received before 5:25pm on 24th May. This gives a window of 10 minutes to instruct validation of the transaction and, thereby, to confirm payment.

If the sender makes a (missed) call to 0320540301 before the expiry time, the transaction proceeds and both the devices 18, 20 of the sender and the recipient are notified accordingly. Exemplary embodiments of the server 12 allow for this to made via a messaging service – e.g. SMS, MMS or equivalent – and, in the event of messaging service notification failure, a call can be made into a helpline IVR (Interactive Voice Response, not shown) where confirmation of the validation of the transaction is made by providing the last transaction from the e-wallet. Optionally, a call centre can easily handle such enquiries either by receiving a call from or placing a call to one or both of the communication devices 18, 20.