UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
18756.37.1
Total Pages in this Submission
4

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111 (a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

and invented by:

Michael A. Liberty

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.:

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 61 pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☒ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity) *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	**Docket No.** *18756.37.1*
	Total Pages in this Submission 4

Application Elements (Continued)

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
   a. ☒ Formal — Number of Sheets 9
   b. ☐ Informal — Number of Sheets _____
4. ☐ Oath or Declaration
   a. ☐ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☐ Copy from a prior application (37CFR 1.63(d) *(for continuation/divisional application only)*
   c. ☐ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. ☒ Application Data Sheet (See 37 CFR 1.76)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. ☐ Assignment Papers *(cover sheet & document(s))*
10. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard *(MPEP 503) (Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Certificate of Mailing
    ☒ Via E-File ☐ Express Mail *(Specify Label No.):* _____

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity) *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. *18756.37.1*
	Total Pages in this Submission 4

Accompanying Application Parts (Continued)

17. ☒ Additional Enclosures *(please identify below):*

This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/562,301, entitled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers", filed on November 21, 2011, which is herein incorporated by reference in its entirety.

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. ☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
18756.37.1
Total Pages in this Submission
4

CLAIMS AS FILED					
For	**#Filed**	**#Allowed**	**#Extra**	**Rate**	**Fee**
Total Claims	20	-20	0	$62.00	$0.00
Indep. Claims	3	-3	0	$250.00	$0.00
Multiple Dependent Claims (check if applicable)					$0.00
Total # of Pages in Specification	61	**Total # of Drawing Sheets**	9		
Total # of Sheets	70			**Application Size Fee**	$0.00
				Basic Fee	$390.00
				Search Fee	$620.00
				Examination Fee	$250.00
OTHER FEE (specify purpose)					
				TOTAL FILING FEE	$1,260.00

☐ A check in the amount of $_____ to cover the filing fee is enclosed.

☒ The Director is hereby authorized to charge and credit Deposit Account No. 23-3178 as described below.

- ☐ Charge the amount of $_____ as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

☒ Payment by credit card.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

/GREGORY R. LUNT/

Signature

Dated: November 19, 2012

Customer Number: 22913

cc:

John C. Stringham
Reg. No. 40,831
Gregory R. Lunt
Reg. No. 57,354
Attorneys for Applicant

P01ULRG/REV09

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	18756.37.1
	Application Number	
Title of Invention	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael	A.	Liberty	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Windermere	State/Province	FL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	5373 Isleworth Country Club Drive		
Address 2			
City	Windermere	State/Province	FL
Postal Code	34786	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22913		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS		
Attorney Docket Number	18756.37.1	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	1	Suggested Figure for Publication (if any)	9

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	18756.37.1
	Application Number	
Title of Invention	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	22913		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61562301	2011-11-21

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	18756.37.1
	Application Number	
Title of Invention	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS	

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Remove

◉	Assignee	○	Legal Representative under 35 U.S.C. 117
○	Person to whom the inventor is obligated to assign.	○	Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :	
If the Assignee is an Organization check here. ☒	
Organization Name	Mozido, LLC

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	18756.37.1
	Application Number	
Title of Invention	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS	

Mailing Address Information:			
Address 1	1950 Stemmons Freeway		
Address 2	Suite 6040		
City	Dallas	**State/Province**	TX
Country [i]	US	Postal Code	75207
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/GREGORY R. LUNT/			Date (YYYY-MM-DD)	2012-11-19
First Name	Gregory	Last Name	Lunt	Registration Number	57354

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

FILED VIA E-FILING

PATENT APPLICATION
Docket No.: 18756.37.1

UNITED STATES PATENT APPLICATION

Of

Michael A. Liberty

For

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/562,301, entitled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers", filed on November 21, 2011, which is herein incorporated by reference in its entirety.

BACKGROUND

[0002] Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BRIEF SUMMARY

[0003] Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

[0004] Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

platform, where the communication indicates confirmation of the processing of the transaction.

[0005] In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0006] In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase.

[0007] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

[0008] Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0010] Figure 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

[0011] Figure 2 illustrates an example embodiment of a cloud-based transaction platform.

[0012] Figures 3A and 3B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

[0013] Figure 4 illustrates an example data flow for making a retail purchase using a mobile wallet.

[0014] Figure 5 illustrates an example embodiment of a monetary transaction system architecture.

[0015] Figure 6 illustrates an alternate example embodiment of a cloud-based transaction platform.

[0016] Figure 7 illustrates an example embodiment data flow for performing a transaction using a third party mobile wallet.

[0017] Figure 8 illustrates an example embodiment data flow for performing a transaction using a third party point of sale (POS) system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[0018] Figure 9 illustrates an example embodiment data flow for making a purchase from a third party mobile wallet provided by a third party mobile wallet provider.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

DETAILED DESCRIPTION

[0019] Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

[0020] Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

platform, where the communication indicates confirmation of the processing of the transaction.

[0021] In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

[0022] In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase. Such purchases may be for items that are provided by the cloud-based transaction platform, either directly or via a third-party provider. These items may include music, movies, games and other downloadable content, physical items that can be shipped to the user and other items such as health care services.

[0023] Embodiments described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

[0024] Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

[0025] A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

[0026] Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

[0027] Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

[0028] Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

[0029] In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[0030] For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

[0031] A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

[0032] Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

[0033] Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

[0034] Various terminology will be used herein to describe the cloud-based transaction platform (also referred to as a “monetary transaction system”, "mobile wallet platform", "mobile wallet program", “mobile wallet transaction system”, "mobile financial services (mFS) platform" or "electronic payment system"). The term “agent” is used to refer to an individual with mFS transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

[0035] The cloud-based transaction platform includes an infrastructure that allows native mobile wallet application and third party mobile wallet applications to interact both with the transaction system and with each other. This allows the user of a native or a third party mobile wallet to make purchases, transfer money or perform any of the other transactions described herein. The cloud-based transaction platform may include a mobile wallet application and a web interface or some other type of

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

functionality that allows the user to interact with the cloud-based transaction platform using their mobile device. The native and third party mobile wallet applications may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

[0036] As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device. The mobile wallet application may either be native (i.e. provided by the provider of the cloud-based transaction platform) or third party (i.e. provided by a provider other than the provider of the cloud-based transaction platform).

[0037] A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices. Any of these applications (or any combination thereof) may be provided on the user's mobile

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

device. This functionality can also be made available on a retail point of sale (POS) system or web site. Indeed, the cloud-based transaction platform allows different POS systems to interact with each other and conduct transactions between themselves.

[0038] The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

[0039] In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

[0040] The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

[0041] The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

[0042] In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued pre-paid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

[0043] The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

[0044] The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[0045] The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

[0046] An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts. The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

[0047] As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney. Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

[0048] The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

[0049] The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

[0050] The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

[0051] The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

numeric password that may be required to perform a transaction via the mobile wallet application.

[0052] The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

[0053] Figure 1 illustrates an example system architecture for a cloud-based transaction platform. Integration tier 101 is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier 101 can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels 111. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") 8583 for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels 111 can be integrated to one or more mechanisms for sending messages to integration

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

tier 101. Notification services 102 is configured to send various notifications through different notification channels 112, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services 102 can be configured through a web services API.

[0054] Service connectors 103 are a set of connectors configure to connect to 3rd party systems 113. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services 104 are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler 105 is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor 121. Payment handler 105 exposes a common API to facilitate interactions with many different kinds of payment processors.

[0055] Security services 106 are configured to perform subscriber authentication. Authorization services 107 are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

[0056] Database 108 is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine 109 is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example,

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

fees and bonuses. Rules engine 109 is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

[0057] Name matching engine 110 is configured to match different objects according to specified configuration rules. Matching engine 110 can be used to find similarities between names, addresses, etc. Transaction processor 121 is configured to manage financial accounts and transactions. The transaction processor 121 can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor 121 can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor 121 can be used to exchange the financial information with a bank.

[0058] Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accorindlgy, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

[0059] The components depicted in Figure 1 can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a third party

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

mobile wallet, adding a debit or credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet (nationally or internationally), making in-store purchases using a third party mobile wallet, selecting health care providers and paying for health care services, paying for music, games, movies or other downloadable provided by a third party provider and made available over the cloud-based transaction system, and various other tasks as described herein below.

[0060] Figure 2 depicts a monetary transaction architecture 200 similar to that described in Figure 1. The monetary transaction architecture 200 may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber 205. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile 211 with the cloud-based transaction system 210. The profile includes the subscriber's know your customer (KYC) information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device 206 such as a phone or tablet. The mobile device runs the native or third party mobile wallet application 207.

[0061] The subscriber can indicate, using the mobile wallet application 207, which transaction or other action he or she would like to perform. The indicated transaction 208 is sent to the mobile wallet platform 210 to be carried out by the platform. The transaction processor 216 (which may be similar to or the same as transaction processor 121 of Figure 1) performs the transaction(s) specified by the (unbanked) subscriber 205. The transaction processor may implement various other

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

components to perform the transaction including memory 217, (wireless) communication module 215, rules engine 220 and/or a transaction database 225.

[0062] Performing the specified transactions may include communicating with the monetary transaction database 225 to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney 221 in his or her stored value account, or has enough money in his or her bank account). Rules engine 220 may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney 221 to or from an entity such as a user or agent (e.g. customer 222) to or from an establishment such as an agent terminal (i.e. a retail store or agent company) 223.

[0063] In some cases, the cloud-based transaction system 210 provides a web interface that allows subscribers of third party mobile wallet applications to perform the same functions provided for native subscribers. For instance, mobile wallet application 207 may provide a web interface that allows a user to enroll for a native or third party mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of communication channels (111 from Figure 1) connected to the cloud-based transaction system 210. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber 205 over at least one of the plurality of communication channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

to activate the (unbanked) subscriber 205 and create a subscriber account for the (unbanked) subscriber.

[0064] Once the subscriber has an account, the cloud-based transaction system generates (or allows the third party provider to generate) a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application). The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the third party or native mobile wallet functionality described herein.

[0065] It should also be noted that the mobile device 206 may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application 207 may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system 200 may be accessed and used via substantially any type of plan-based or prepaid mobile device.

[0066] The components depicted in Figure 1 can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a third party mobile wallet, adding a stored value account (either hosted by an electronic payment system or a third party), adding a bank/credit union account to a third party mobile wallet, adding a debit/credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet, making in store purchases from a third party mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in Figure 4).

[0067] Figure 3A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (301) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor 216 of the monetary transaction system 210 determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system 210 decrements subscriber A's account and credits subscriber B's account (302). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two cloud-based platform subscribers, one or both of which may be unbanked. The cloud-based transaction system 210 processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

[0068] Figure 3B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic 305, subscriber A wishes to send eMoney to

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

another individual that is not a subscriber to the cloud-based transaction platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the cloud-based transaction system 210 cannot credit them with eMoney. Instead, the cloud-based transaction system 210 sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (306). The cloud-based transaction system 210 puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system 210.

[0069] When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the cloud-based transaction platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (307) and the user leaves with the cash in hand (308). The cloud-based transaction platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

[0070] Figure 4 illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the cloud-based transaction platform and are able to accept native and third party mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system 210 then debits the subscriber's eMoney account (401) and credits the agent branch's eMoney account (402). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a cloud-based transaction platform-specified bank.

[0071] In one embodiment, the cloud-based transaction system 210 is implemented to make a purchase from a mobile wallet. The communications module 215 of the monetary transaction system 210 receives a communication from a subscriber over a communication channel 111. The subscriber communication indicates that an unbanked subscriber 205 desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's native or third party mobile wallet.

[0072] The monetary transaction system 210 then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch). The monetary transaction system 210 validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the selected payment method, debits the specified payment method by the specified amount of funds, returns a notification to the agent branch

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

authorizing the purchase and sends a receipt to the unbanked subscriber over a communication channel. The cloud-based transaction system 210 may thus be used in this manner to make a retail purchase using a native or third party mobile wallet.

[0073] Figure 5 depicts a physical environment and corresponding computer system architecture 500 for allowing a user to participate in various services using a native or third party mobile wallet (e.g. 511). Some of these services include allowing the user 507 to access disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The environment 500, like the scenarios described in Figures 3A, 3B and 4, involves the use of a native or third party mobile wallet application 511. The mobile wallet application 511 can be used to provide disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The mobile wallet application may be run on any type of digital device including a mobile phone, tablet, laptop or other digital device. Embodiments include providing digital data (e.g., coupons or vouchers) for obtaining disruptively priced or free items (e.g., consumer goods or groceries) to such digital devices.

[0074] In some embodiments, a user has an account with a mobile payment system. The cloud-based transaction system (e.g. 210 of Figure 2 or electronic payment system 521 of Figure 5) can provide the user 507 with a variety of functionality including purchasing items (see Figure 4), depositing funds, withdrawing funds, transferring funds (see Figures 3A and 3B), and others all from a third party wallet. Accordingly, the user can use a digital device to interact with the electronic payment system 521 to pay for goods and/or services.

[0075] In exchange for some type of financial benefit, the user opts in to receive advertisements. The financial benefits may include coupons, vouchers, promotions,

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Buy One Get One ("BOGO") offers or any other type of benefit (such as a reduced cost or free financial service or good) from the electronic payment system. The benefit may be targeted to the user based on the user's age, location or other demographic information, or based on the user's past purchases. At least in some embodiments, when the user agrees to participate in opt-in advertising, the electronic payment system 521 is permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains lists of the users' purchased items in a data warehouse. The electronic payment system may also store information about the user (anonymous or otherwise) including age, income level, an indication of whether kids are in the family, or other information that may be useful in targeting ads or benefits to the user.

[0076] The electronic payment system analyzes 534 the users purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The advertisements and/or promotions can be for items the user has purchased 503. The advertisements and/or promotions can also be for items related to items the user has purchase. For example, if user has purchased a particular brand of razor, advertisements for the brand's shaving cream can be identified. Advertisements for related items can also be used for cross-promotion.

[0077] From time to time, at specified intervals, or based on location (e.g., having a coupon for a merchant this is with a specified proximity) the electronic payment system sends identified advertisements and/or promotions to the user's digital device. When specified advertising thresholds are satisfied (e.g., a specified number and/or type of advertisements and/or promotions are presented), the electronic payment system confers a financial benefit on the user's account. For example, the electronic

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

payment system can provide the user's account with a low cost (e.g., reduced fee) or free financial service, such as, for example, one reduced cost bill pay or one free bill pay. Alternately, the electronic payment system can provide the user's account with a coupon or voucher for an item (e.g., an item a user has pre-selected or an item the user has purchased in the past).

[0078] In some embodiments, a client application for the electronic payment system runs on the user's digital device (e.g. mobile wallet application 511). The user interacts with the electronic payment system through the client application. From a screen of the client application, the user can agree to accept opt in advertising. Accordingly, embodiments of the invention essentially permit a user to self-monetize themselves through their digital device.

[0079] As further depicted in Figure 5, computer architecture 500 includes digital device 508, retail location 502, and electronic payment system 521. Digital device 508 further includes mobile wallet application 511. Retail location 502 further includes its own mobile wallet application 512. Electronic payment system 521 includes marketing module 533, data warehouse 532, advertisements 538, payment processor 522, user mobile wallet 524 (user 507's mobile wallet), and merchant mobile wallet 526 (retail location 502's mobile wallet).

[0080] Generally, each company in packaged goods companies 571 (or retailers that sell the packaged goods or other goods or services) can send advertisement data to electronic payment system 521. Advertisements 538 represent the collection of advertisement data sent from packaged goods companies 571. Each company in packaged goods companies 571 can also submit benefit rules to electronic payment system 521. Benefit rules 578 represent the collection of benefit rules sent from packaged goods companies 571. Benefit rules 578 define when a benefit, such as, for

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

example, a free financial service, a coupon, a promotion, etc, is to be granted to a user of electronic payment system 521. For example, in response to completing a questionnaire linked to a product advertisement, a user can be given a coupon for the product or for a related product.

[0081] In general, user 507 can use native or third party mobile wallet application 511 to pay for goods purchased at retail location 502 (as shown in Figure 4). For example, user 507 can use mobile wallet application 511 to purchase goods 503. To pay for goods 503, mobile wallet application 511 can send payment instruction 543 in amount 563 to electronic payment system 521. Payment processor 522 can receive payment instruction 543. In response, payment processor 522 can debit 541 user mobile wallet 524 by amount 563. Payment processor 522 can also credit 542 merchant mobile wallet 526 by amount 563.

[0082] User 507 can use mobile wallet application 511 to participate in opt-in advertising. For example, user 507 can use mobile wallet application 511 to send opt-in 544 to electronic payment system 521. Advertising module 533 can receive opt-in 544 and record that mobile wallet application 511 has opted in for advertising. As such, when user 507 makes a purchase using mobile wallet application 511, a list of purchased items is sent to electronic payment system 521. For example, upon purchasing goods 503, item list 531 is sent to electronic payment system 521 and stored in data warehouse 532.

[0083] Propensity analysis module 534 can analyze user 507's purchases, including item list 531. From the analysis, propensity analysis module 534 can identify items or categories of items user 507 may be interested in. The items can be items user 507 has purchased in the past (e.g., an item in goods 503) or items related to items user 507 has purchases in the past. Propensity analysis module 534 can

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

indicate identified items or categories of items to advertisement identification module 536. These identified items or categories are items that the user is likely interested in and, as such, may have a propensity toward buying these items. The propensity analysis module may use past purchases, personal preferences, lifestyle or demographic information or other data in the propensity analysis.

[0084] Advertisement identification module 536 can then select advertisements from advertisements 538 that correspond to the identified items or categories of items. For example, advertisement identification module 536 can select advertisement 546 for presentation at mobile wallet application 511. Advertisement 546 can be an advertisement for a product made by a company in packaged goods companies 571. Additionally or alternatively, the advertisement 546 may be created by the merchant and may advertise products or services sold by that merchant.

[0085] Advertising module 533 can send selected advertisements to mobile wallet application 511. For example, advertising module 533 can send advertisement 546 (e.g., related to an item in goods 503) to mobile wallet application 511. In general, advertisements can include interactive content. For example, advertisement 546 includes content 573. Content 573 can be a video, a link to a company website (e.g., for a company in packaged goods companies 571), a call to action (such as a questionnaire), or some other content user 507 can interact with through digital device 508. User 507 can interact with content 573, for example, responding to questions in content 573. Advertisement response 574 can indicate how user 507 has interacted with content 573. In one embodiment, a call to action may be to post an update on Facebook® or some other website such as a retail establishment ranking website. If the user makes such a post or performs some other call to action, the user may be

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

rewarded with a benefit. That benefit may be related to the product about which the user posted on the various websites.

[0086] Based on advertisement response 574, benefit determination module 576 can determine if a benefit is to be conferred upon user 507. Benefit determination module 576 can refer to benefit rules 578 when making a determination whether or not to confer a benefit. Thus, when user 507 interacts with advertisement 546 in a specified way (e.g., completes a survey, watches a video, etc.), benefit rules 578 can indicate that a company benefit (e.g., benefit 577) is to be conferred upon user 507. For example, benefit determination module 576 can confer benefit 577 on user 507. When user 507 receives an advertisement for a razor, for instance, and answers a questionnaire on how often they shave, a razor manufacture can give user 507 a coupon for reduced cost or free razor blades.

[0087] When a benefit is to be conferred on a user, the benefit can be stored in the user's brand locker. For example, benefit determination module 576 can store benefit 577 in brand locker 572 (part of user mobile wallet 524). Benefit 577 can be a coupon, a reduced cost or free financial service, a voucher, a promotion, a free bill pay, etc.

[0088] Benefit determination module 576 can also track aggregate statistics, such as, for example, specified number and/or type of advertisements received, for advertisements presented at native or third party mobile wallet application 511. Benefits can also be conferred upon users based on the aggregate statistics. For example, benefit determination module 576 can confer a benefit upon user 507 in response to twenty advertisements being presented at mobile wallet application 511. Thus, conferred benefits can be company-specified benefits or can be electronic payment system-specified benefits. Electronic payment system 521 can notify a user

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

when a benefit is conferred. For example, electronic payment system 521 can send benefit notification 547 to mobile wallet application 511 to indicate benefit 577 being stored in brand locker 572.

[0089] When user 507 makes subsequent purchases through user mobile wallet 524, electronic payment system 521 can automatically check brand locker 572 for benefits related to any purchases items. If benefits for an item are identified, user 507 can be notified through mobile wallet application 511. In some cases, if benefits are identified, those benefits can be applied automatically when the user purchases that item or service. Thus, if the benefit is a coupon or a buy one get one free offer, that benefit may be applied automatically when the user uses his or her mobile wallet application 511 to purchase that item. Accordingly, embodiments of the invention permit user 507 to self monetize digital device 508 through agreeing to participate in opt-in advertising.

[0090] Although not depicted, various other modules from the architecture of Figures 1 or 2 can also be included electronic payment system 521. The modules expressly depicted in Figure 5 can interoperate with these other modules as appropriate to facilitate desired functionality.

[0091] Figures 7-9 will now be described in conjunction with the computer architecture 600 illustrated in Figure 6. Figure 6 depicts a mobile wallet platform 601 that may have an architecture as shown in Figure 1. As further depicted in Figure 6, mobile wallet platform 601 communicates with an agent terminal 602 or a customer 607 to process transactions using a native or third party mobile wallet 605. Mobile wallet platform 601 may also communicate with a third party processor 604 to process transactions using a mobile wallet or third party mobile wallet. Mobile wallet platform 601 may also communicate with a third party mobile wallet platform 603 to

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

process transactions using a mobile wallet owned or managed by a third party mobile wallet provider.

[0092] Mobile wallet platform 601 may also process the mobile wallet transaction or third party mobile wallet transaction internally, without the use of third party processors or third party mobile wallet platforms. In particular, mobile wallet platform 601 may process transactions using third party mobile wallets in the same or similar manner that transactions are processed as shown in Figures 2-5. Accordingly, the physical environment and corresponding computer system architecture 600 shown in Figure 6 allows a cloud-based transaction platform 601 to support multiple third party mobile wallet providers.

[0093] Mobile wallet platform 601 communicates with agent terminal 602, third party mobile wallet platform 603, third party processor 604, and customer's mobile phone 619 through a variety of communication channels. For example, the communication between mobile wallet platform 601 and any one of these entities may be through communication channels 111, notification channels 112, or third party systems 113, as shown in Figure 1. Communication between mobile wallet platform 601 and any one of these entities may also be through processor 121 shown in Figure 1.

[0094] With respect to the entire description of Figure 6, and as explained above, the term "mobile wallet" encompasses not only mobile wallets owned or managed by the mobile wallet platform, but also third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. In contrast, the term "third party mobile wallet" refers only to third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. Accordingly, cloud-based transaction platform 601 may manage and

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

process transactions using mobile wallets 605, which may be mobile wallets owned by cloud-based transaction platform 601 or mobile wallets owned by a third party mobile wallet provider.

[0095] As shown in Figure 6, customer 607 initiates a mobile wallet transaction 608 at agent terminal 602. Agent terminal 602 may be part of an agent network consisting of one or more agent terminals that communicate with cloud-based transaction platform 601. Examples of agent terminals are stores and other commercial establishments. Alternatively, customer 607 may initiate a mobile wallet transaction 609 by communicating with cloud-based transaction platform 601 through a channel selected by the customer.

[0096] Mobile wallet transactions 608 and 609 may be one or more of any type of transaction that can be performed using a mobile wallet, including but not limited to, a deposit, withdrawal, transfer, purchase, bill payment, topping up of a prepaid mobile account, or any other transaction described herein. Customer 607 may initiate transactions 608 and 609 in a variety of ways. For example, customer 607 can initiate a deposit into a mobile wallet, a withdrawal from a mobile wallet, a bill payment from a mobile wallet, topping up of a prepaid mobile account using a mobile wallet, a transfer from a mobile wallet, a remittance transaction, a selection of health care provider or payment of health services, a purchase of music, movies, games or other downloadable content, or other purchases using a mobile wallet.

[0097] After customer 607 initiates transaction 609 through agent terminal 602, agent terminal 602 then communicates with cloud-based transaction platform 601 by sending transaction data 610 to cloud-based transaction platform 601. Once cloud-based transaction platform 601 has received the transaction either through transaction data 610 from agent terminal 602 or from transaction 609 initiated by customer 607,

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

cloud-based transaction platform 601 may then process the transaction in a variety of ways.

[0098] For example, cloud-based transaction platform 601 may process the transaction by communicating with third party processor 604 by sending third party transaction data 611, which may include some or all of the information in transaction data 610. Third party processor can then perform the requested transactional processing and respond by sending confirmation data 612 to cloud-based transaction platform 601. Confirmation data 612 can indicate whether the requested mobile wallet transaction was processed successfully or unsuccessfully.

[0099] In another example, cloud-based transaction platform 601 may process the transaction by communicating with third party mobile wallet platform 603 by sending third party transaction data 613, which may include some or all of the information in transaction data 610. Third party mobile wallet platform 603 may have any architecture which is suitable for processing mobile wallet transactions. Third party mobile wallet platform 603 may have an architecture that is the same or similar to the architecture shown in Figure 1.

[00100] Alternatively, third party mobile wallet platform 603 may have a different architecture. In addition, any aspects of cloud-based transaction platform 601 or functionality provided by that platform may also be present in third party mobile wallet platform 603. After receiving third party transaction data 613, third party mobile wallet platform 603 may process the transaction itself or forward the transaction to third party processor 604 by sending third party transaction data 614.

[00101] Once processing of the transaction is complete, third party mobile wallet platform 603 may respond to cloud-based transaction platform 601 by sending confirmation data 615. Confirmation data 615 can indicate whether the requested

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

mobile wallet transaction was processed successfully or unsuccessfully. In addition, following the processing performed by third party mobile wallet platform 603 after receiving third party transaction data 613, the third party mobile wallet platform 603 may provide a commission or transaction fee 616 to cloud-based transaction platform 601.

[00102] In a further example, mobile wallet platform 601 may process the transaction internally within cloud-based transaction platform 601. Specifically, cloud-based transaction platform 601 may process a transaction using a third party mobile wallet entirely within cloud-based transaction platform 601.

[00103] Once processing of the transaction is complete, cloud-based transaction platform 601 may communicate with agent terminal 602 by sending confirmation data 617 indicating information such as whether the transaction was successful or not. Also following processing of the transaction, mobile wallet platform may send customer notification 618 through an appropriate channel such as to the customer's mobile phone 619. For example, customer notification 618 may be sent using the notification services 102 and notification channels 112 (e.g. SMPP, SMTP, voice) of Figure 1.

[00104] With reference now to Figures 2, 6 and 7, the cloud-based transaction system 210 receives communication 226 from an agent terminal 223 over a communication channel connected to the cloud-based transaction platform 210/601 (act 710). The agent communication indicates that a customer 222/205 desires to perform a mobile wallet transaction using their third party mobile wallet 207. The cloud-based transaction system 210 sends the agent communication to a third party mobile wallet platform 603 (act 720). The cloud-based transaction system 210 then receives communication 611 from the third party mobile wallet platform confirming

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

processing of the transaction 612 (act 730) and sends communication 617 to the agent terminal 602 over communication channels 111 connected to the cloud-based transaction platform indicating confirmation of the processing of the transaction (act 740).

[00105] As mentioned above, multiple different types of transactions may be performed using the infrastructure provided by the cloud-based transaction system. The transactions may be a performed not only by a first customer that uses a first mobile wallet provider, but also by a second, different customer using a second, different third party mobile wallet provider. The third party mobile wallet platform may use a third party processor to perform (at least parts of) the transaction. The customer may be notified of confirmation of the processing of the transaction using the third party mobile wallet over various communication channels connected to the cloud-based transaction platform. In some cases, each third party mobile wallet provider has their own point of sale (POS) processing system 230. The third party mobile wallet providers' POS processing systems may communicate with each other using the cloud-based transaction platform to process the transaction.

[00106] One of the transactions made possible by the cloud-based transaction platform 601 is depositing funds into a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction system may receive a communication 226 from the agent terminal 223 over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that the customer desires to deposit a specified amount of funds into their third party mobile wallet 605. The cloud-based transaction system may then credit the third party mobile wallet with the specified amount of funds.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[00107] Another transaction provided by the cloud-based transaction platform 601 is withdrawing funds from a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction platform receives communication 208 from the customer 205 indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet. The cloud-based transaction platform 601 returns a secure, perishable withdrawal code to the customer over at least one of the communication channels connected to the cloud-based transaction platform. It also receives communication from the agent terminal 223 indicating that the withdrawal code has been presented to an agent and debits the third party mobile wallet by the specified amount of funds.

[00108] Another transaction provided by the cloud-based transaction platform 601 is transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider. In this transaction, the platform 601 receives a customer communication 208 indicating that a customer 205 desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet 606. The cloud-based transaction platform debits the third party mobile wallet by the specified amount of funds and transfers the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient. The specified amount of funds is then transferred to the second third party mobile wallet platform.

[00109] Yet another transaction provided by the cloud-based transaction platform 601 is making a purchase from a third party mobile wallet managed by a third party mobile wallet platform. In this transaction, the cloud-based transaction platform

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

receives communication 208 from the customer 205 indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet 606. The cloud-based transaction platform returns a secure, perishable purchase code to the customer, receives communication 226 from the agent terminal 223 indicating that the purchase code has been presented to an agent, and debits the customer's third party mobile wallet by the specified amount of funds.

[00110] In another embodiment, as shown in Fig. 8, a cloud-based transaction system performs or facilitates a transaction using a third party point of sale (POS) system. The cloud-based transaction system receives communication 226 from a specified POS system 224 implemented at an agent terminal 223 over a communication channels 111 connected to the cloud-based transaction platform 210 (act 810). The POS communication indicates that a customer 205 has initiated a mobile wallet transaction using their third party mobile wallet 207. The cloud-based transaction system sends the POS communication to a corresponding third party POS transaction processing system 230 that has been established to process POS transactions from the specified POS system (act 820). The cloud-based transaction system then receives communication from the third party POS transaction processing system 230 confirming processing of the transaction (act 830) and sends communication to the specified POS system 224 implemented at the agent terminal 223 indicating confirmation of the processing of the transaction (act 840).

[00111] In some cases, transaction fees or commissions 616 may be paid by the third party mobile wallet platform to the cloud-based transaction platform for facilitating the transaction. One of the transactions allowed by the cloud-based transaction system is depositing funds into a third party mobile wallet provided by a

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

third party mobile wallet provider. In this transaction, the cloud-based transaction platform 210 receives communication 226 from a specified POS system 224 implemented at the agent terminal 223 over a communication channels 111 connected to the cloud-based transaction platform. The POS communication indicates that the customer 205/222 desires to deposit a specified amount of funds into the third party mobile wallet 606 provided by the third party mobile wallet provider. The cloud-based transaction system validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the specified POS system implemented at the agent terminal is authorized to deposit money, performs a limit check or a velocity check on the third party mobile wallet provided by the third party mobile wallet provider, credits the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds, returns a notification to the specified POS system implemented at the agent terminal confirming the deposit and notifies the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over a communication channel connected to the cloud-based transaction platform 210.

[00112] Another transaction provided by the cloud-based transaction platform 210 is withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform 210 receives communication 208 from a customer 205 indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet 606 provided by the third party mobile wallet provider. The cloud-based transaction platform 210 validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

withdrawal for the specified amount of funds, performs a limit check and/or a velocity check on the third party mobile wallet, returns a secure, perishable withdrawal code to the customer over a communication channel 111 connected to the cloud-based transaction platform, receives subsequent POS communication 226 indicating that the withdrawal code has been presented to an agent (e.g. at agent terminal 223), debits the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds, returns a notification to the POS system at the agent terminal confirming the withdrawal and notifies the customer 205 (e.g. in confirmation 617) that the specified amount of funds were withdrawn from the third party mobile wallet.

[00113] In yet another transaction provided by the cloud-based transaction platform, money is transferred using a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform 210 receives customer communication 208 indicating that the customer 205 desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet 606, where the transfer uses a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform 210. The cloud-based transaction platform validates the status of the specified payment method, performs a limit check and/or a velocity check on the specified payment method, performs a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control, debits the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds, transfers the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the specified recipient over a communication channel connected between the cloud-based transaction platform and the third party mobile wallet provider, and

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

notifies the customer that the specified amount of funds was transferred to the specified recipient.

[00114] In another transaction provided by the cloud-based transaction platform 210, a purchase is made from a third party mobile wallet provided by a third party mobile wallet provider. In this transaction, the cloud-based transaction system receives communication 208 from the customer 205 indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet 606. The cloud-based transaction system returns a secure, perishable purchase code to the customer, receives subsequent agent terminal communication indicating that the purchase code has been presented to an agent, validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the specified payment method, debits the customer's third party mobile wallet by the specified amount of funds by sending communication to the third party mobile wallet provider, returns a notification to the POS system at the agent terminal authorizing the purchase and sends a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

[00115] Figure 9 describes a further embodiment in which a cloud-based transaction platform facilitates making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction system 210 receives communication 208 from a customer 205 over a communication channel connected to the cloud-based transaction platform (act 910). The customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

party mobile wallet 606. The cloud-based transaction system returns a secure, perishable purchase code to the customer (act 920) and receives communication from an agent terminal 223 over at least one of the communication channels connected to the cloud-based transaction platform indicating that the purchase code has been presented to an agent (act 930). The cloud-based transaction system 210 then debits the customer's third party mobile wallet 606 by the specified amount of funds (act 940).

[00116] Substantially any item may be purchased using this transaction technique including items provided directly by the cloud-based transaction system, or items provided by third party retailers through the cloud-based transaction system. These items may include health care services, physical, shippable items, music, games, movies or any other digital or downloadable content.

[00117] Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the United States by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and U.S. PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, First Name, Last Name, Date of Birth, Government ID Type, Government ID Number, Address. The CIP processes are designed to validate customer identity against government blacklists and assist in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

[00118] Non-Documentary Verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis. Documentary Verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Various differ forms of identification including Driver's license, Passport, Alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

[00119] Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

[00120] The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

CLAIMS

What is claimed:

1. A cloud-based transaction platform including:

one or more processors;

system memory;

one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a third party mobile wallet, the method comprising the following:

an act of receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a mobile wallet transaction using their third party mobile wallet;

an act of sending the agent communication to a third party mobile wallet platform;

an act of receiving communication from the third party mobile wallet platform confirming processing of the transaction; and

an act of sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

2. The cloud-based transaction platform of claim 1, wherein a transaction is performed by a second, different customer using a second, different third party mobile wallet.

3. The cloud-based transaction platform of claim 1, wherein the third party mobile wallet platform comprises a third party processor.

4. The cloud-based transaction platform of claim 1, wherein the transaction using a third party mobile wallet comprises one or more of a deposit, a withdrawal, a transfer, a purchase, a bill payment, or topping up of a prepaid mobile account.

5. The cloud-based transaction platform of claim 1, further comprising an act of notifying the customer of confirmation of the processing of the transaction using the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

6. The cloud-based transaction platform of claim 1, wherein the third party mobile wallet is provided by a third party mobile wallet provider.

7. The cloud-based transaction platform of claim 1, wherein each third party mobile wallet provider has their own point of sale (POS) processing system.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

8. The cloud-based transaction platform of claim 7, wherein the third party mobile wallet providers' POS processing systems communicate with each other using the cloud-based transaction platform to process the transaction.

9. The cloud-based transaction platform of claim 1, wherein the transaction comprises depositing funds into a third party mobile wallet owned by an entity different than the customer, including:

an act of receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into their third party mobile wallet; and

an act of crediting the third party mobile wallet with the specified amount of funds.

10. The cloud-based transaction platform of claim 1, wherein the transaction comprises withdrawing funds from a third party mobile wallet owned by an entity different than the customer, including:

an act of receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet;

an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

an act of receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the withdrawal code has been presented to an agent; and

an act of debiting the third party mobile wallet by the specified amount of funds.

11. The cloud-based transaction platform of claim 6, wherein the transaction comprises transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider, the method comprising:

an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet;

an act of debiting the third party mobile wallet by the specified amount of funds; and

an act of transferring the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the second third party mobile wallet platform.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

12. The cloud-based transaction platform of claim 1, wherein the transaction comprises making a purchase from a third party mobile wallet managed by a third party mobile wallet platform, including:

an act of receiving communication from the customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet;

an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform;

an act of receiving communication from the agent terminal over at least one of the plurality of channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent; and

an act of debiting the customer's third party mobile wallet by the specified amount of funds.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

13. A cloud-based transaction platform including:

one or more processors;

system memory;

one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for performing a transaction using a third party point of sale (POS) system, the method comprising:

an act of receiving communication from a specified POS system implemented at an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that a customer has initiated a mobile wallet transaction using their third party mobile wallet;

an act of sending the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system;

an act of receiving communication from the third party POS transaction processing system confirming processing of the transaction; and

an act of sending communication to the specified POS system implemented at the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction.

14. The cloud-based transaction platform of claim 13, further comprising the act of receiving a transaction fee paid by the specified POS system to the cloud-based transaction platform.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

15. The cloud-based transaction platform of claim 13, wherein the transaction comprises depositing funds into a third party mobile wallet provided by a third party mobile wallet provider, including:

an act of receiving communication from the specified POS system implemented at the agent terminal over one of the plurality of channels connected to the cloud-based transaction platform, the POS communication indicating that the customer desires to deposit a specified amount of funds into the third party mobile wallet provided by the third party mobile wallet provider;

an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider;

an act of determining if the specified POS system implemented at the agent terminal is authorized to deposit money;

an act of performing one or more of a limit check and a velocity check on the third party mobile wallet provided by the third party mobile wallet provider;

an act of crediting the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds;

an act of returning a notification to the specified POS system implemented at the agent terminal confirming the deposit; and

an act of notifying the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

16. The cloud-based transaction platform of claim 13, wherein the transaction comprises withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider, including:

an act of receiving communication from a customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet provided by the third party mobile wallet provider;

an act of validating the status of the third party mobile wallet provided by the third party mobile wallet provider;

an act of determining if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds;

an act of performing one or more of a limit check and a velocity check on the third party mobile wallet;

an act of returning a secure, perishable withdrawal code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform;

an act of receiving subsequent POS communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the POS communication indicating that the withdrawal code has been presented to an agent;

an act of debiting the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

an act of returning a notification to the POS system at the agent terminal confirming the withdrawal; and

an act of notifying the customer that the specified amount of funds were withdrawn from the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

17. The cloud-based transaction platform of claim 13, wherein the transaction comprises transferring money using a third party mobile wallet provided by a third party mobile wallet provider, including:

an act of receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet, the transfer using a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform;

an act of validating the status of the specified payment method;

an act of performing one or more of a limit check and a velocity check on the specified payment method;

an act of performing a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control;

an act of debiting the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds;

an act of transferring the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

specified recipient over at least one of the plurality of channels connected between the cloud-based transaction platform and the third party mobile wallet provider;

an act of notifying the customer that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the cloud-based transaction platform.

18. The cloud-based transaction platform of claim 13, wherein the transaction comprises making a purchase from a third party mobile wallet provided by a third party mobile wallet provider, including:

an act of receiving communication from the customer over one of the plurality of communication channels connected to the mobile wallet platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet;

an act of returning a secure, perishable purchase code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform;

an act of receiving subsequent agent terminal communication over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent;

an act of validating the status of the specified payment method;

an act of determining if the specified payment method can accommodate a purchase for the specified amount;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

an act of performing one or more of a limit check and a velocity check on the specified payment method;

an act of debiting the customer's third party mobile wallet by the specified amount of funds by sending communication to the third party mobile wallet provider;

an act of returning a notification to the POS system at the agent terminal authorizing the purchase; and

an act of sending a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

19. A cloud-based transaction platform including:

one or more processors;

system memory;

one or more computer-readable storage media having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the computing system to perform a method for making a purchase from a third party mobile wallet provided by a third party mobile wallet provider, the method comprising the following:

an act of receiving communication from a customer over one of a plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet;

an act of returning a secure, perishable purchase code to the customer over at least one the plurality of communication channels connected to the cloud-based transaction platform;

an act of receiving communication from an agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent; and

an act of debiting the customer's third party mobile wallet by the specified amount of funds.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

20. The cloud-based transaction platform of claim 19, wherein the item purchased by the customer comprises at least one of the following: health care services, music, games, and movies.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

ABSTRACT

Embodiments are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one scenario, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

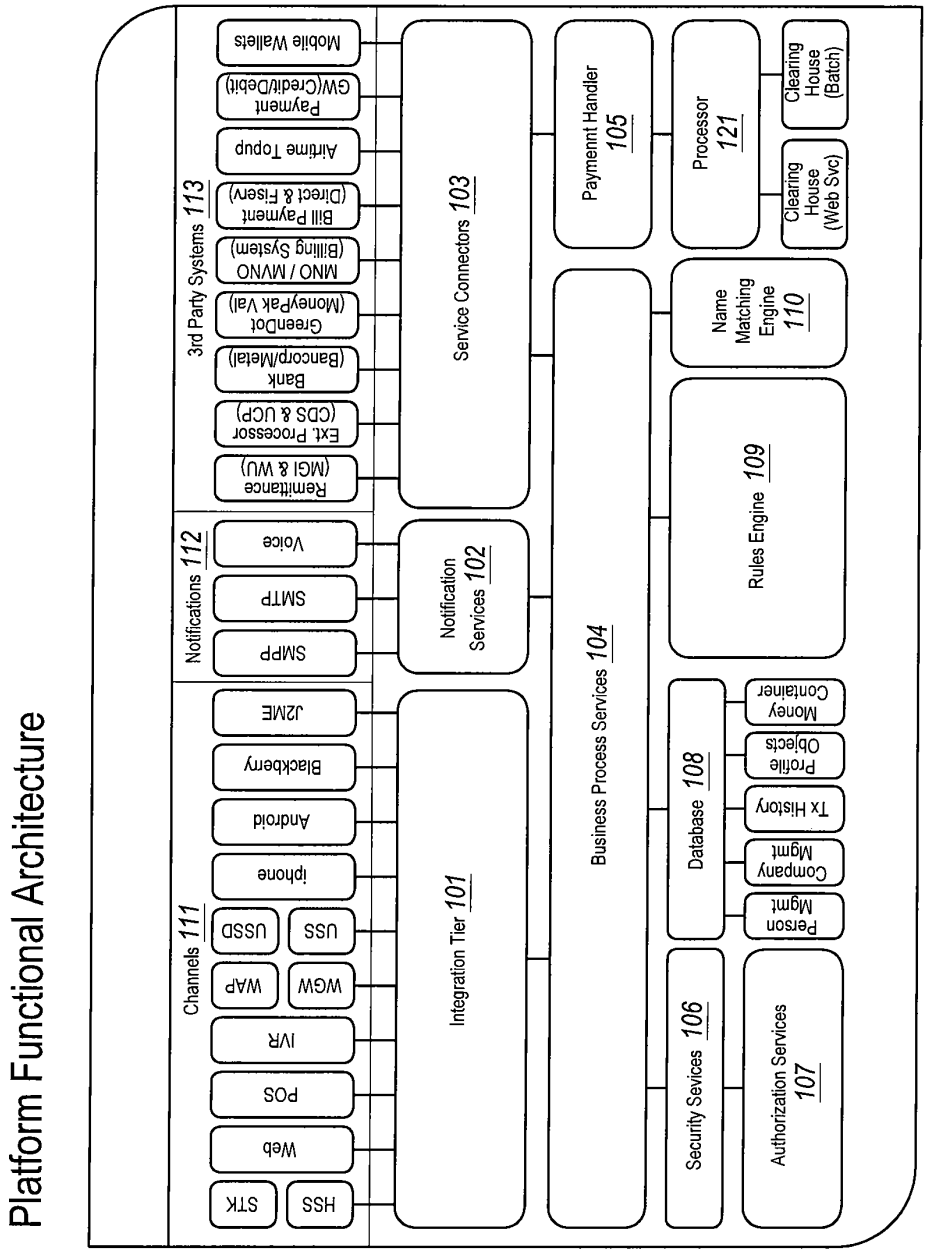

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USSD
USS
iphone
Android
Blackberry
J2ME
Notifications 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Metal)
GreenDot (MoneyPak Val)
MNO / MVNO (Billing System)
Bill Payment (Direct & Fiserv)
Airtime Topup
Payment GW(Credit/Debit)
Mobile Wallets
Integration Tier 101
Notification Services 102
Service Connectors 103
Business Process Services 104
Paymennt Handler 105
Security Sevices 106
Authorization Services 107
Database 108
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Rules Engine 109
Name Matching Engine 110
Processor 121
Clearing House (Web Svc)
Clearing House (Batch)

FIG. 1

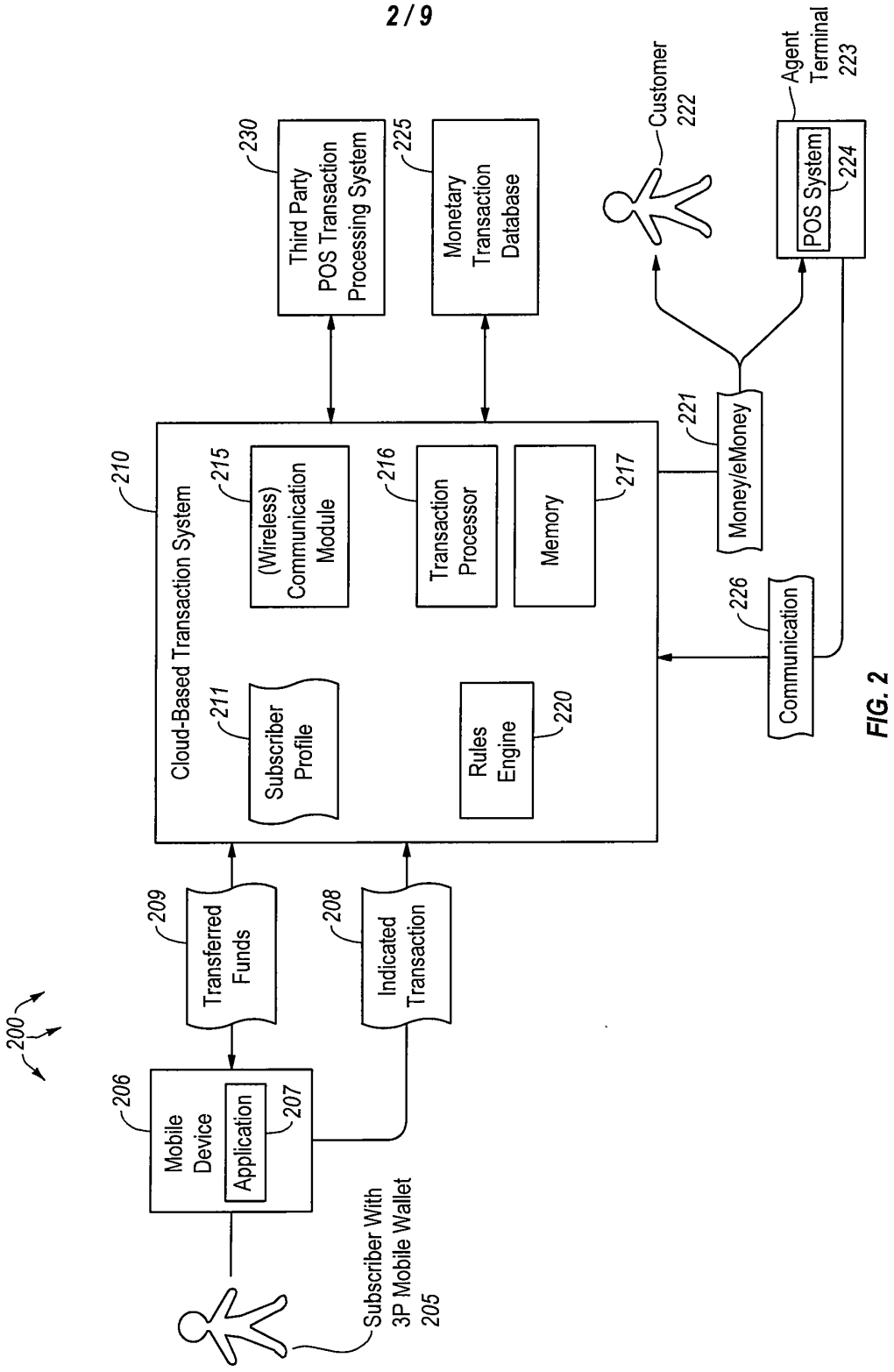

200
Subscriber With 3P Mobile Wallet 205
Mobile Device 206
Application 207
Transferred Funds 209
Indicated Transaction 208
Cloud-Based Transaction System 210
Subscriber Profile 211
(Wireless) Communication Module 215
Transaction Processor 216
Memory 217
Rules Engine 220
Money/eMoney 221
Communication 226
Third Party POS Transaction Processing System 230
Monetary Transaction Database 225
Customer 222
Agent Terminal 223
POS System 224

FIG. 2

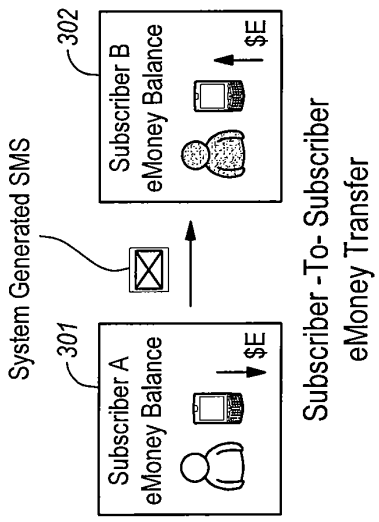

System Generated SMS
301
Subscriber A
eMoney Balance
$E
302
Subscriber B
eMoney Balance
$E
Subscriber -To- Subscriber
eMoney Transfer

FIG. 3A

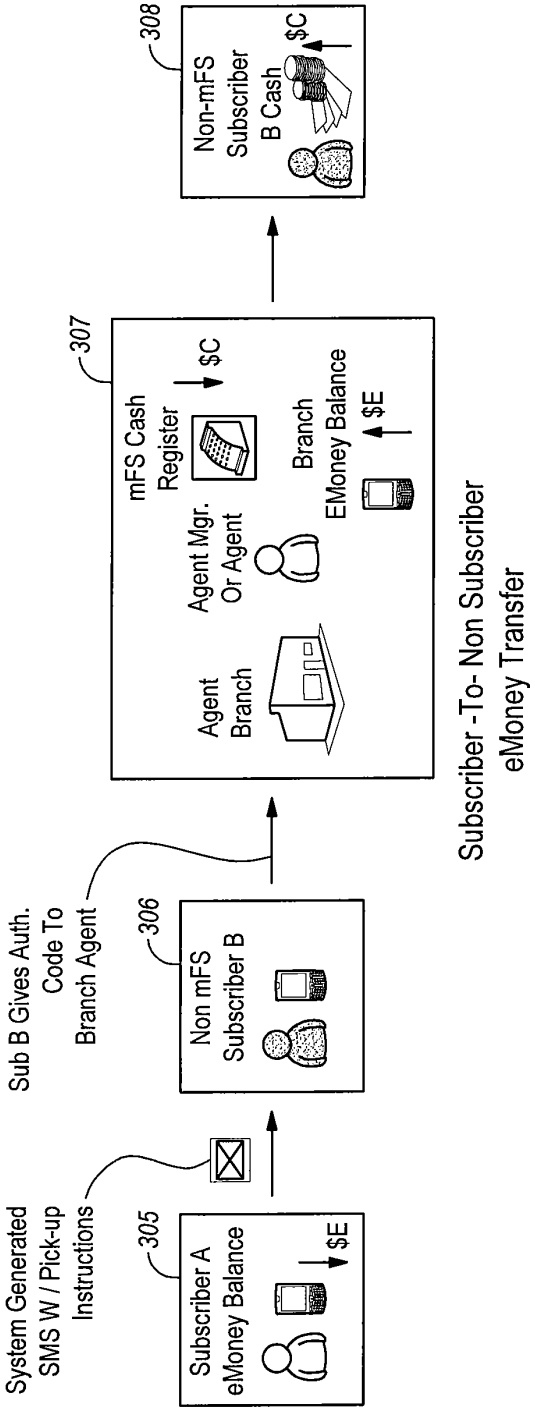
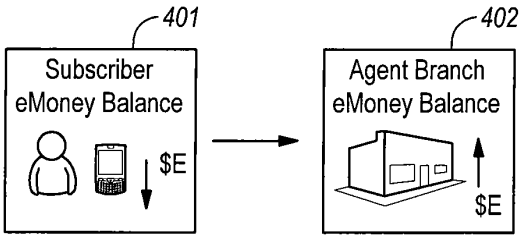

System Generated
SMS W / Pick-up
Instructions
305
Subscriber A
eMoney Balance
$E
Sub B Gives Auth.
Code To
Branch Agent
306
Non mFS
Subscriber B
307
Agent
Branch
Agent Mgr.
Or Agent
mFS Cash
Register
$C
Branch
EMoney Balance
$E
308
Non-mFS
Subscriber
B Cash
$C
Subscriber -To- Non Subscriber
eMoney Transfer

FIG. 3B



Subscriber Makes Retail Purchase

FIG. 4

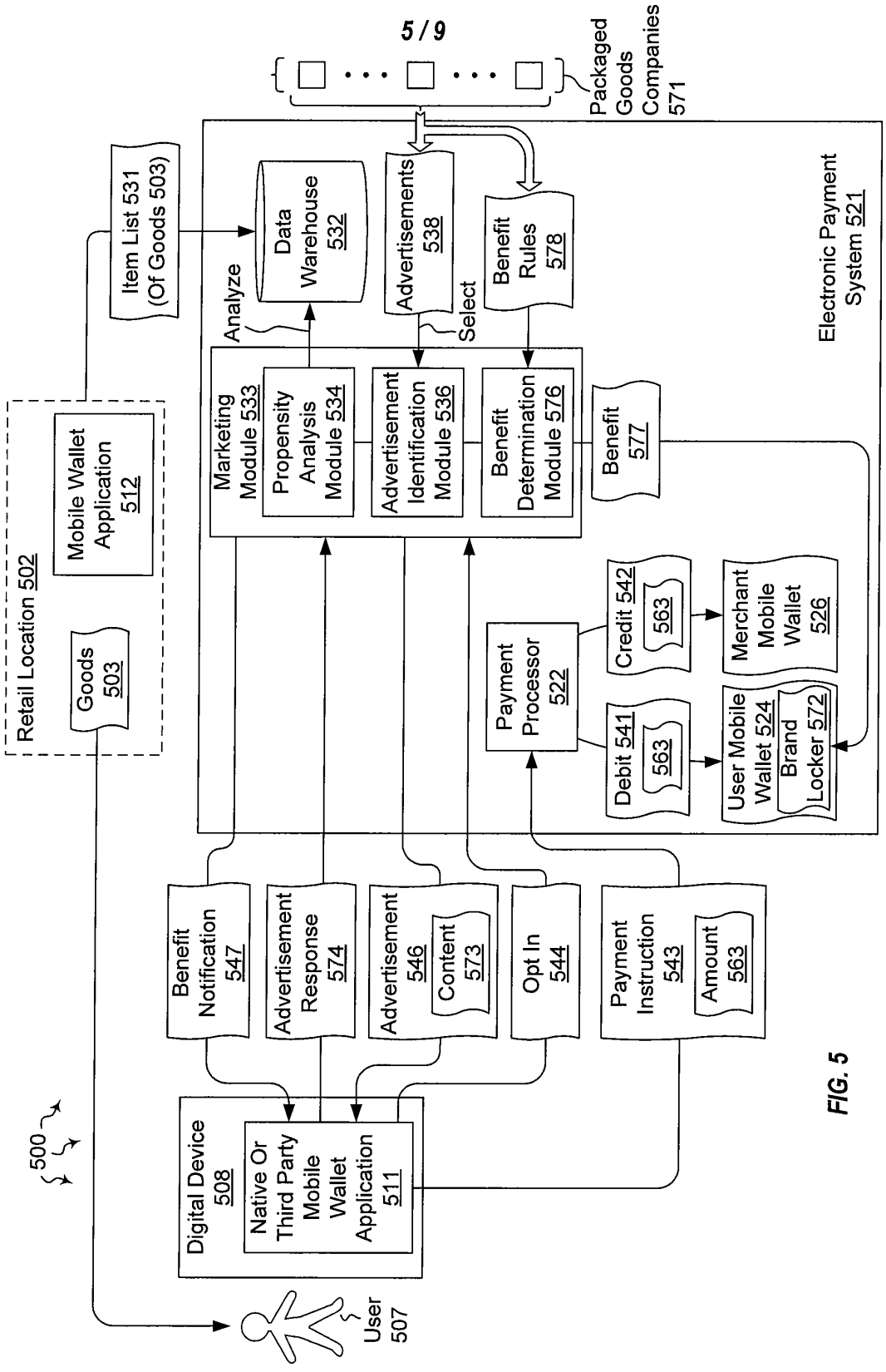

Packaged Goods Companies 571
Item List 531 (Of Goods 503)
Data Warehouse 532
Advertisements 538
Benefit Rules 578
Analyze
Select
Electronic Payment System 521
Marketing Module 533
Propensity Analysis Module 534
Advertisement Identification Module 536
Benefit Determination Module 576
Benefit 577
Retail Location 502
Mobile Wallet Application 512
Goods 503
Payment Processor 522
Credit 542
563
Merchant Mobile Wallet 526
Debit 541
563
User Mobile Wallet 524
Brand Locker 572
Benefit Notification 547
Advertisement Response 574
Advertisement 546
Content 573
Opt In 544
Payment Instruction 543
Amount 563
500
Digital Device 508
Native Or Third Party Mobile Wallet Application 511
User 507

FIG. 5

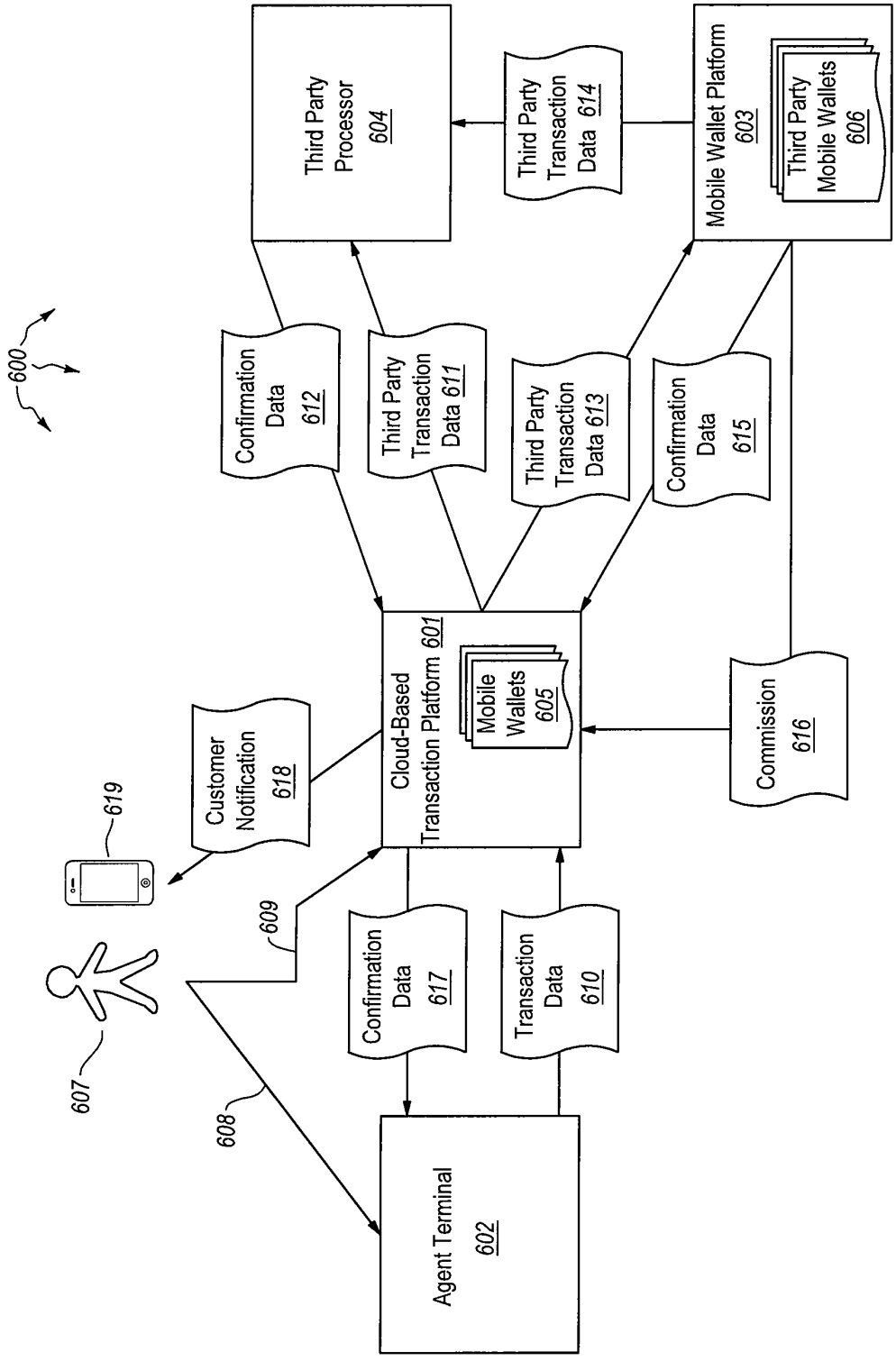

600
Third Party Processor 604
Third Party Transaction Data 614
Mobile Wallet Platform 603
Third Party Mobile Wallets 606
Confirmation Data 612
Third Party Transaction Data 611
Third Party Transaction Data 613
Confirmation Data 615
Cloud-Based Transaction Platform 601
Mobile Wallets 605
Customer Notification 618
Commission 616
619
609
Confirmation Data 617
Transaction Data 610
607
608
Agent Terminal 602

FIG. 6

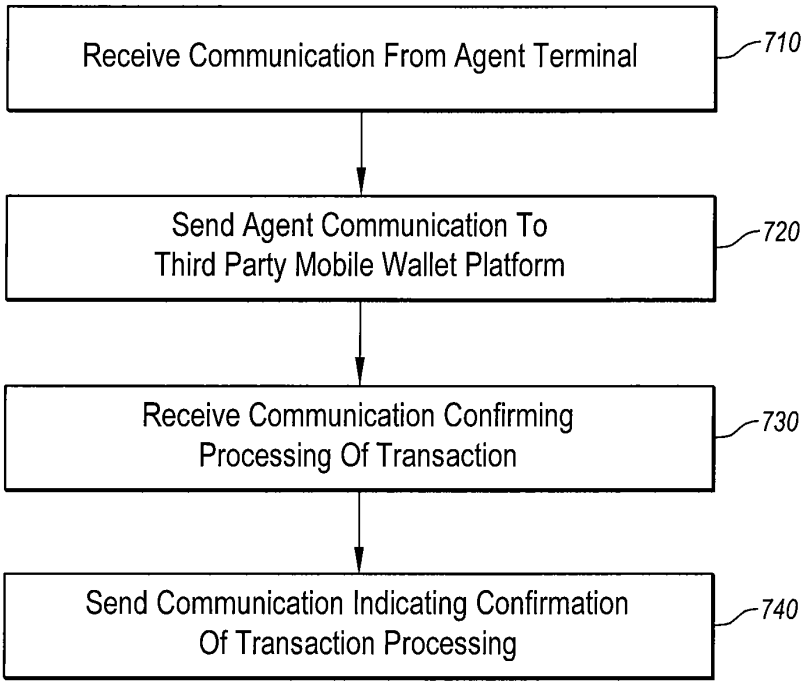

Receive Communication From Agent Terminal
710
Send Agent Communication To Third Party Mobile Wallet Platform
720
Receive Communication Confirming Processing Of Transaction
730
Send Communication Indicating Confirmation Of Transaction Processing
740

FIG. 7

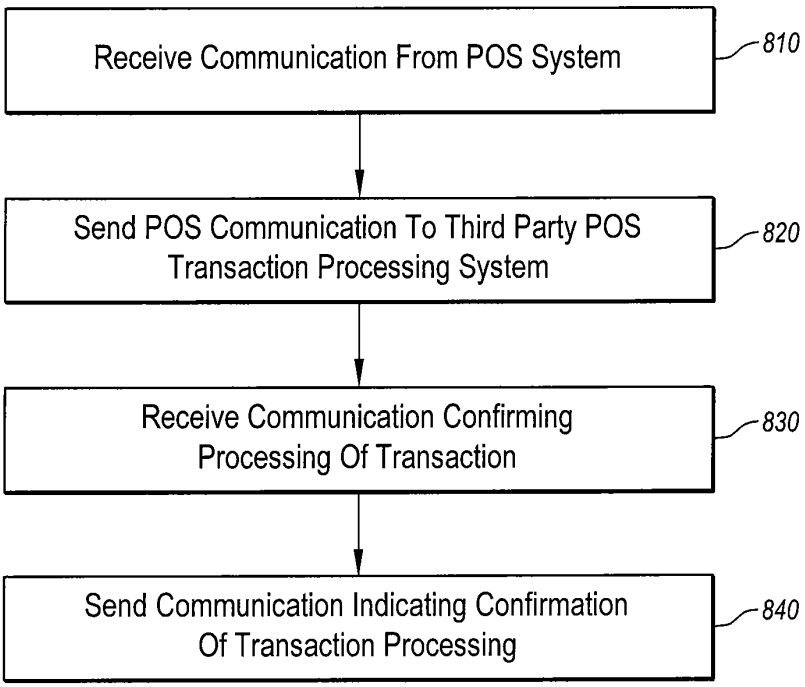

Receive Communication From POS System
810
Send POS Communication To Third Party POS Transaction Processing System
820
Receive Communication Confirming Processing Of Transaction
830
Send Communication Indicating Confirmation Of Transaction Processing
840

FIG. 8

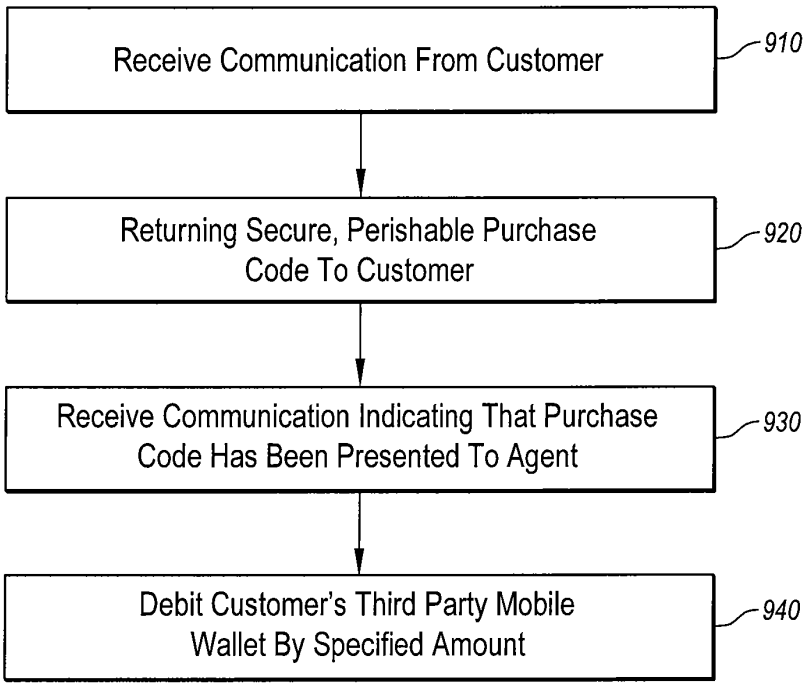

Receive Communication From Customer
910
Returning Secure, Perishable Purchase Code To Customer
920
Receive Communication Indicating That Purchase Code Has Been Presented To Agent
930
Debit Customer's Third Party Mobile Wallet By Specified Amount
940

FIG. 9

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS
First Named Inventor/Applicant Name:	Michael A. Liberty
Filer:	GREGORY LUNT/Connie Boulton
Attorney Docket Number:	18756.37.1

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	390	390
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1260**

Electronic Acknowledgement Receipt

EFS ID:	14262895
Application Number:	13680824
International Application Number:	
Confirmation Number:	7971
Title of Invention:	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	GREGORY LUNT/Connie Boulton
Filer Authorized By:	GREGORY LUNT
Attorney Docket Number:	18756.37.1
Receipt Date:	19-NOV-2012
Filing Date:	
Time Stamp:	16:32:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1260
RAM confirmation Number	4334
Deposit Account	233178
Authorized User	LUNT, GREGORY

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Transmittal.pdf	402264 7546e8bb051e69ba3530e4d7354ad686d75c555a	no	4
Warnings:					
Information:					
2	Application Data Sheet	ADS.pdf	1395811 d01575d1b1e68e94d27161ff17ab4d1be30f6c61	no	5
Warnings:					
Information:					
3		Application.pdf	539872 b0da9fb95a1d98b8dbbe46c65df89eabdb0e5c03	yes	61

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	47
Claims	48	60
Abstract	61	61

Warnings:					
Information:					
4	Drawings-only black and white line drawings	Figures.pdf	198845 7a63a7677bf84afe4f593bd5ab57daae9da33eb3	no	9
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	33438 336eebfce0862591c8211bf6cb5fb786d6a6eea6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2570230		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Michael A. Liberty
Application No.: 13/680,824
Filed: November 19, 2012
Customer No.: 22913
Title:

Attorney Docket No.: 18756.37.1
Group Art Unit: Not Yet Assigned
Confirmation Number: 7971
Examiner: Not Yet Assigned

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

STATEMENT FILED PURSUANT TO
THE DUTY OF DISCLOSURE UNDER 37 C.F.R. §§ 1.56, 1.97 AND 1.98

Sir:

Pursuant to the duty of disclosure under 37 C.F.R. §§ 1.56, 1.97 and 1.98, the Applicant requests consideration of this Information Disclosure Statement.

PART I: Compliance with 37 C.F.R. § 1.97

This Information Disclosure Statement has been filed within three (3) months of the filing date of a National Application.

No fee or certification is required.

PART II: Additional Information

The Applicant hereby makes the following additional information of record in the above-identified application.

Serial No.	Filing Date	Inventor(s)
N/A	N/A	N/A

PART III: Remarks

The Applicant hereby makes of record in the above-identified application the information listed on the attached form PTO/SB/08A. The order of presentation of the references should not be construed as an indication of the importance of the references. Documents cited on the attached form PTO/SB/08A are enclosed unless otherwise indicated. It is respectfully requested that:

1. The Examiner consider completely the cited information, along with any other information, in reaching a determination concerning the patentability of the present claims;

2. The enclosed form PTO/SB/08A be signed by the Examiner to evidence that the cited information has been fully considered by the Patent and Trademark Office during the examination of this application;

3. The citations for the information be printed on any patent which issues from this application.

By submitting this Information Disclosure Statement, the Applicant makes no representation that a search has been performed, of the extent of any search performed, or that more relevant information does not exist.

By submitting this Information Disclosure Statement, the Applicant makes no representation that the information cited in the Statement is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

By submitting this Information Disclosure Statement, the Applicant makes no representation that the information cited in the Statement is, or is considered to be, in fact, prior art as defined by 35 U.S.C. § 102.

Notwithstanding any statement by the Applicant, the Applicant urges the Examiner to form his own conclusion regarding the relevance of the cited information.

An early and favorable action is hereby requested.

Respectfully submitted,

Date December 3, 2012

By/GREGORY R. LUNT/

Reg. No. 57,354

CERTIFICATE OF MAILING OR TRANSMISSION
(Under 37 CFR § 1.8(a)) or ELECTRONIC FILING

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

December 3, 2012
Date

/GREGORY R. LUNT/
Signature

Gregory R. Lunt
Printed Name

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7248855		2007-07-24	Joyce et al.	
	2	7275685		2007-10-02	Gray et al.	
	3	7822688		2010-10-26	Labrou et al.	
	4	8160959		2012-04-17	Rackley, III et al.	
	5	7699218		2010-04-20	Garcia et al.	
	6	6714797		2004-03-30	Rautila	
	7	7461010		2008-12-02	Kwan	
	8	7107247		2006-09-12	Kinoshita et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	9	6185545		2001-02-06	Resnick et al.	
	10	7100821		2006-09-05	Rasti	
	11	8016185		2011-09-13	Modi	
	12	7677973		2010-03-16	Van Luchene	
	13	6957342		2005-10-18	Vantanen	
	14	7774231		2010-08-10	Pond et al.	
	15	5828739		1998-10-27	Nakanishi	
	16	7240836		2007-07-10	Vrotsos et al.	
	17	6415156		2002-07-02	Stadelmann	
	18	7069001		2006-06-27	Rupp et al.	
	19	7089208		2006-08-08	Levchin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	20	7099850		2006-08-29	Mann, II et al.	
	21	7347361		2008-03-25	Lovett	
	22	7494055		2009-02-24	Fernandes et al.	
	23	7461028		2008-12-02	Wronski, Jr.	
	24	7657489		2010-02-02	Stambaugh	
	25	7708194		2010-05-04	Vawter	
	26	7958052		2011-06-07	Powell	
	27	8095113		2012-01-10	Kean et al.	
	28	7988060		2011-08-02	Killian et al.	
	29	7865414		2011-01-04	Fung et al.	
	30	7024174		2006-04-04	Nagy et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	31	7784684		2010-08-31	Labrou et al.	
	32	7606560		2009-10-20	Labrou et al.	
	33	8073783		2011-12-06	Felsted et al.	
	34	5991749		1999-11-23	Morrill, Jr.	
	35	8052042		2011-11-08	Kolinski-Schultz et al.	
	36	5717374		1998-02-10	Smith	
	37	8090945		2012-01-03	Singhal	
	38	7877605		2011-01-25	Labrou et al.	
	39	7801826		2010-09-21	Labrou et al.	
	40	7822688		2010-10-26	Labrou et al.	
	41	7353382		2008-04-01	Labrou et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	42	7349871		2008-03-25	Labrou et al.	
	43	7363261		2008-04-22	Whitehead, Jr. et al.	
	44	7729963		2010-06-01	Lego et al.	
	45	7937302		2011-05-03	Lego et al.	
	46	7937305		2011-05-03	Lego et al.	
	47	7729987		2010-06-01	Wakim et al.	
	48	7890424		2011-02-15	Wakim et al.	
	49	7110972		2006-09-19	Handa et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020052754		2002-05-02	Joyce et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	2	20060179452		2006-08-10	Amodeo et al.	
	3	20070244811		2007-10-18	Tumminaro	
	4	20070255653		2007-11-01	Tumminaro et al.	
	5	20120095856		2012-04-19	Sanjeev	
	6	20120245986		2012-09-27	Regan et al.	
	7	20070106564		2007-05-10	Matotek et al.	
	8	20090157546		2009-06-18	Garcia et al.	
	9	20090177578		2009-07-09	Garcia et al.	
	10	20090177581		2009-07-09	Garcia et al.	
	11	20090254479		2009-10-08	Pharris	
	12	20090254440		2009-10-08	Pharris	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	13	20090281904		2009-11-12	Pharris	
	14	20120047070		2012-02-23	Pharris	
	15	20030071115		2003-04-17	Horn et al.	
	16	20020069123		2002-06-06	Soderlind et al.	
	17	20030154165		2003-08-14	Horn et al.	
	18	20070179885		2007-08-02	Bird et al.	
	19	20060287004		2006-12-21	Fuqua	
	20	20030001010		2003-01-02	Schmidt et al.	
	21	20050199709		2005-09-15	Linlor	
	22	20020152177		2002-10-17	Wolf	
	23	20040248554		2004-12-09	Khan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	24	20080011825		2008-01-17	Giordano et al.	
	25	20020161708		2002-10-31	Offer	
	26	20020131404		2002-09-19	Mehta et al.	
	27	20050070265		2005-03-31	Korpinen	
	28	20070033285		2007-02-08	Shiigi	
	29	20070244811		2007-10-18	Tumminaro	
	30	20020042776		2002-04-11	Woo et al.	
	31	20020065774		2002-05-30	Young et al.	
	32	20030195842		2003-10-16	Reece	
	33	20050222961		2005-10-06	Staib et al.	
	34	20060136901		2006-06-22	Nichols	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	35	20060200427		2006-09-07	Morrison et al.	
	36	20070125838		2007-06-07	Law et al.	
	37	20070125840		2007-06-07	Law et al.	
	38	20070203850		2007-08-30	Singh et al.	
	39	20080017704		2008-01-24	VanDeburg et al.	
	40	20080040285		2008-02-14	Wankmueller	
	41	20080208743		2008-08-28	Arthur et al.	
	42	20080208744		2008-08-28	Arthur et al.	
	43	20080208762		2008-08-28	Arthur et al.	
	44	20080210751		2008-09-04	Kim	
	45	20080249928		2008-10-09	Hill et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	46	20080255947		2008-10-16	Friedman	
	47	20080275779		2008-11-06	Lakshminarayanan	
	48	20090108015		2009-04-30	Kreamer	
	49	20090138366		2009-05-28	Bemmel et al.	
	50	20090144161		2009-06-04	Fisher	
	51	20090248537		2009-10-01	Sarkeshik	
	52	20100044430		2010-02-25	Song et al.	
	53	20100057619		2010-03-04	Weller et al.	
	54	20100063895		2010-03-11	Dominguez et al.	
	55	20090063312		2009-03-05	Hurst	
	56	20090222353		2009-09-03	Guest et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	57	20090106148		2009-04-23	Prada	
	58	20050080697		2005-04-14	Foss, Jr. et al.	
	59	20110313924		2011-12-22	Carell et al.	
	60	20100197326		2010-08-05	Ngo	
	61	20040235450		2004-11-25	Rosenberg	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	102073958	CN		2011-05-25	TIANJIN ZTE SOFTWARE CORP		☐
	2	0171627	WO		2001-09-27	QUALCOMM INCORPORATED		☐
	3	2003012717	WO		2003-02-13	C-SAM, INC.		☐
	4	2004010393	WO		2004-01-29	PARTNER COMMUNICATIONS COMPANY LTD.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	5	2004023353	WO		2004-03-18	TYNEVALE PTY LIMITED		☐
	6	2004088641	WO		2004-10-14	WAY SYSTEMS, INC.		☐
	7	2004053640	WO		2004-06-24	WAY SYSTEMS, INC.		☐
	8	9913636	WO		1999-03-18	TEKTON COMMUNICATIONS LIMITED		☐
	9	2002071354	WO		2002-09-12	SOFT TRACKS ENTERPRISES LTD		☐
	10	2001357164	JP		2001-12-26	NTT DATA CORP		☐
	11	2001097118	WO		2001-12-20	JOGU		☐
	12	199834203	WO		1998-08-06	QUALCOMM INCORPORATED		☐
	13	2005079254	WO		2005-09-01	FUJITSU LIMITED		☐
	14	2005086593	WO		2005-09-22	A LITTLE WORLD PRIVATE LIMITED		☐
	15	2007145500	WO		2007-12-21	MOBILE MONEY INTERNATIONAL SDN BHD		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	16	2008008735	WO		2008-01-17	IBREVA CORPORATION		☐
	17	101606400	CN		2009-12-16	DELOITTE SERVICES PTY LTD		☐
	18	2666616	CA		2008-04-24	FRUITFUL TECHNOLOGIES PTY LTD, AU		☐
	19	2007312879	AU		2008-04-24	FRUITFUL TECHNOLOGIES PTY LTD.		☐
	20	2084921	EP		2008-04-24	FRUITFUL TECHNOLOGIES PTY LTD.		☐
	21	1280115	EP		2003-01-29	NTT DOCOMO, INC.		☐
	22	10-2007-0092400	KR		2007-09-13	SHIN H. BANK		☐
	23	10-2003-0068603	KR		2003-08-25	NARU SYSTEM CO.		☐
	24	10-2002-0065989	KR		2002-08-14	STARBRIDGE COMMUNICATIONS CO., LTD.		☐
	25	10119808	DE		2002-09-12	HOLLAND CHRIS		☐
	26	2002-99716	JP		2002-04-05	KUNINOBU MASANAO		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

	27	2001297198	JP		2001-10-26	MIWA GINKO KK [MIWAN]		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	CHEN, Jiajun Jim et al. Short-range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th international conference on Electronic commerce [Online] 2004, pp. 649-656.	☐
	2	LABROU, Yannis et al. Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.	☐
	3	MOTOROLA, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (accessed October 4, 2012).	☐
	4	VALCOURT, E. et al., "Investigating Mobile Payment", Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on 22-24 Aug. 2005, August 2005, Volume 4, pages 29-36 Vol. 4.	☐
	5	GAO, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System", Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) July 2005, 10 pages.	☐
	6	EDWIN, et al., "Technobiography", October 2004, 29 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13680824
	Filing Date	2012-11-19
	First Named Inventor	Michael A. Liberty
	Art Unit	
	Examiner Name	
	Attorney Docket Number	18756.37.1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GREGORY R. LUNT/	Date (YYYY-MM-DD)	2012-12-03
Name/Print	Gregory R. Lunt	Registration Number	57354

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	14342613
Application Number:	13680824
International Application Number:	
Confirmation Number:	7971
Title of Invention:	USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS
First Named Inventor/Applicant Name:	Michael A. Liberty
Customer Number:	22913
Filer:	GREGORY LUNT/Connie Boulton
Filer Authorized By:	GREGORY LUNT
Attorney Docket Number:	18756.37.1
Receipt Date:	03-DEC-2012
Filing Date:	
Time Stamp:	17:22:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	For_Ref_2003012717.pdf	2355356 b77744635cdc1b1ec0f7aad968c79e278d8b8e96	no	62

Warnings:	
Information:	

2	Foreign Reference	For_Ref_2004010393.pdf	989487 88f9dcbc2987f187b1b1192d64d1409ca059f3e3	no	22
Warnings:					
Information:					
3	Foreign Reference	For_Ref_AU2007312879.pdf	5311333 7bce47da68a70a84ba9e34c3170efe6ba83645ea	no	85
Warnings:					
Information:					
4	Foreign Reference	For_Ref_CA26666616.pdf	2795889 daa750b78d33ca81231415ba10c0ef28574eb8a8	no	84
Warnings:					
Information:					
5	Foreign Reference	For_Ref_Cn101606400.pdf	44396 7922fe04f14604eda789f613f13c2a400e0ca9fd	no	1
Warnings:					
Information:					
6	Foreign Reference	For_Ref_CN102073958.pdf	821322 5b8a2224ed5d36abbb4e174e7871007d18e052af	no	14
Warnings:					
Information:					
7	Foreign Reference	For_Ref_DE10119808.pdf	168191 d3711c2c496ece3275d8bf56bb06d5bf9a54b035	no	1
Warnings:					
Information:					
8	Foreign Reference	For_Ref_EP1280115.pdf	2108721 413b58cdca1b89370241be155340459fbf348c0b	no	45
Warnings:					
Information:					
9	Foreign Reference	For_Ref_EP2084921.pdf	5312263 833f16d67ce5598d639f45f89f5bffd83fcfdacd	no	85
Warnings:					
Information:					
10	Foreign Reference	For_Ref_JP200299716.pdf	202638 e7cfdab57f6a55335ef05ecd8adacbef5c336a5a	no	1
Warnings:					
Information:					

11	Foreign Reference	For_Ref_JP2001297198.pdf	442270 e2edb853e60ea1eb341c08191f39b03a93d104df	no	8
Warnings:					
Information:					
12	Foreign Reference	For_Ref_JP2001357164.pdf	82000 6bf878c817960cea248b2167967224d9b9d04e6a	no	2
Warnings:					
Information:					
13	Foreign Reference	For_Ref_KR1020020065989.pdf	56331 ae48dd5ffdeb28e1412b10dce58935171ea4392f	no	2
Warnings:					
Information:					
14	Foreign Reference	For_Ref_KR1020030068603.pdf	53135 b3cf7394f0d69acbd666c88ca101522083b95fa1	no	2
Warnings:					
Information:					
15	Foreign Reference	For_Ref_KR1020070092400.pdf	53124 b40f74689b79ee728524a8124f7e8f0e6aaabd0d	no	2
Warnings:					
Information:					
16	Foreign Reference	For_Ref_WO0171627.pdf	1369949 8d9dae2176f899cf3dce25e8ae97fde1366389f7	no	35
Warnings:					
Information:					
17	Foreign Reference	For_Ref_WO9913636.pdf	1620533 cf3a45959ed2bb8ace48baeeadc73f4cbad2c4ef	no	48
Warnings:					
Information:					
18	Foreign Reference	For_Ref_WO199834203.pdf	1647270 33ac3ebd62557b47af5861af879ba9fbd8445ddb	no	40
Warnings:					
Information:					
19	Foreign Reference	For_Ref_WO2001097118.pdf	7393956 fe645ab2507db8d2a44206f30bb2e4e65510763e	no	163
Warnings:					
Information:					

20	Foreign Reference	For_Ref_WO2002071354.pdf	1253948 72547b8aefd8bcead3c98dac93bb50c682ce5ced	no	31
Warnings:					
Information:					
21	Foreign Reference	For_Ref_WO2004023353.pdf	3691947 23ca75305bc8fb641d4192566053393acdb40042	no	70
Warnings:					
Information:					
22	Foreign Reference	For_Ref_WO2004053640.pdf	2571305 a33886d4137fca21aae235f66476407f183d70b9	no	41
Warnings:					
Information:					
23	Foreign Reference	For_Ref_WO2004088641.pdf	1668825 b1a50792c70fdb211894eecdacea135b8420d582	no	34
Warnings:					
Information:					
24	Foreign Reference	For_Ref_WO2005079254.pdf	3553344 69ec8f59ebeb819fb475c15a57fa7740c2449820	no	63
Warnings:					
Information:					
25	Foreign Reference	For_Ref_WO2005086593.pdf	899960 cb70c22e9c66a770967e5bc68fbc93e1619dc08f	no	23
Warnings:					
Information:					
26	Foreign Reference	For_Ref_WO2007145500.pdf	1307435 23487921a61b15e4181b837d00e7589a60fb1b9b	no	31
Warnings:					
Information:					
27	Foreign Reference	For_Ref_WO2008008735.pdf	1805135 6bd0789864b071ff0fac344160516bd03d0ff2f3	no	33
Warnings:					
Information:					
28	Non Patent Literature	NPL_Chen.pdf	574879 145de5a2230157e4d2e67549afb51be41740cb67	no	8
Warnings:					
Information:					

29	Non Patent Literature	NPL_Edwin.pdf	1542743 ff33406c7443012f920db1ef7d3292a10882b21b	no	29
Warnings:					
Information:					
30	Non Patent Literature	NPL_Gao.pdf	940035 9dcabe8f1898dcf41ec12c4e52e23c0819c1c877	no	10
Warnings:					
Information:					
31	Non Patent Literature	NPL_Labrou.pdf	903475 25f3cdbf4a03e5224d18106f45609c856e84e78f	no	10
Warnings:					
Information:					
32	Non Patent Literature	NPL_Motorola.pdf	1175314 d9ce9f9934767b2f4545406790d8fc95ad56111e	no	4
Warnings:					
Information:					
33	Non Patent Literature	NPL_Valcourt.pdf	535905 cccb44080167 30ca838eae98c67542aa7f25eb3d	no	8
Warnings:					
Information:					
34	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	626678 fd1147c4eabe22e58bd3167d9c0d74fec9e46cd4	no	20
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
			Total Files Size (in bytes):	55879092	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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

(19) World Intellectual Property Organization
International Bureau

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

PCT

(10) International Publication Number
WO 03/012717 A1

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

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

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

(25) Filing Language: English

(26) Publication Language: English

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

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

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

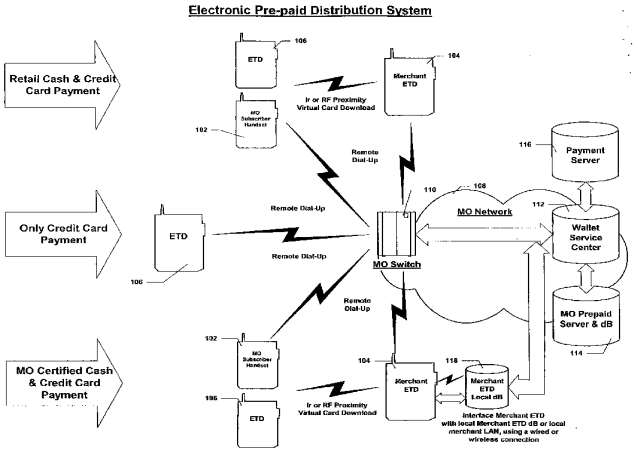
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU,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

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

Published:
— *with international search report*

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

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



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

WO 03/012717 A1

SYSTEM FOR DISTRIBUTION AND USE OF VIRTUAL STORED VALUE CARDS

BACKGROUND OF THE INVENTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

APPL-1002
APPLE INC. / Page 144 of 1892

What is claimed is:

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

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

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

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

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

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

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

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

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

APPL-1002
APPLE INC. / Page 145 of 1892

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

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

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

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

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

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

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

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

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

a) creating a virtual pre-paid card;

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

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

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

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

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

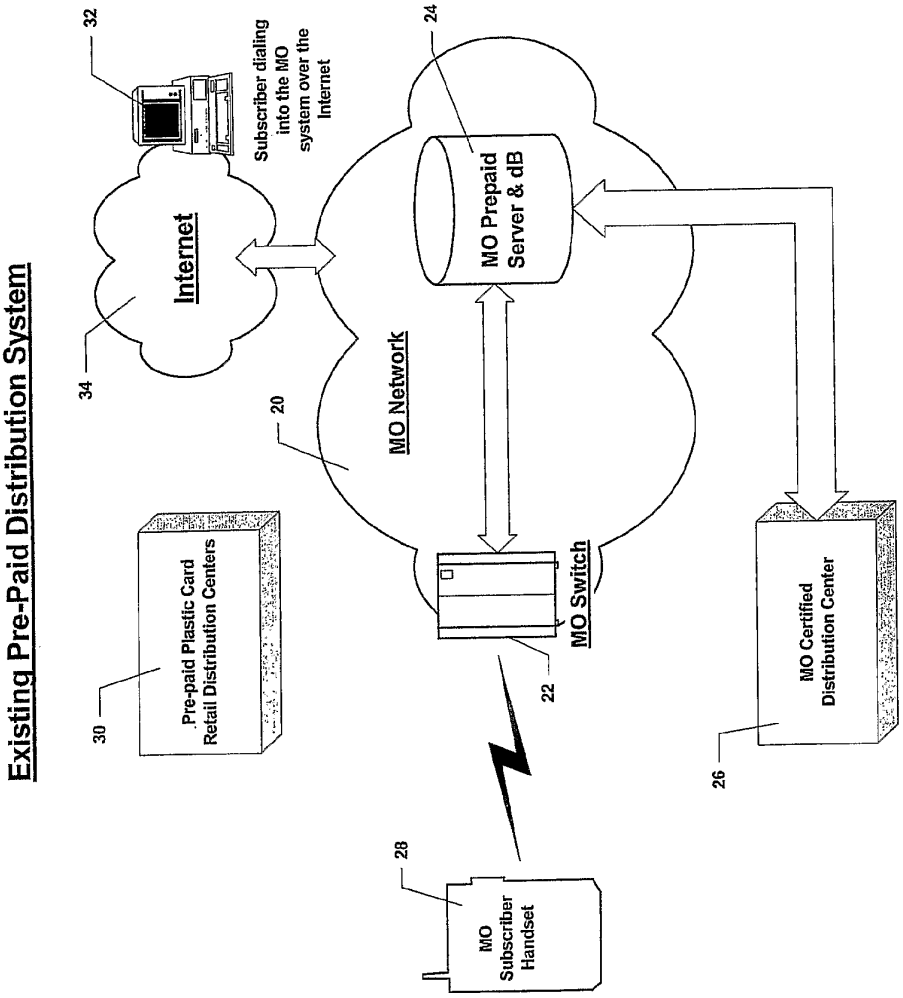
a) transferring payment information and subscriber information from the MO subscriber handset to the retailer electronic transaction device; and

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

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

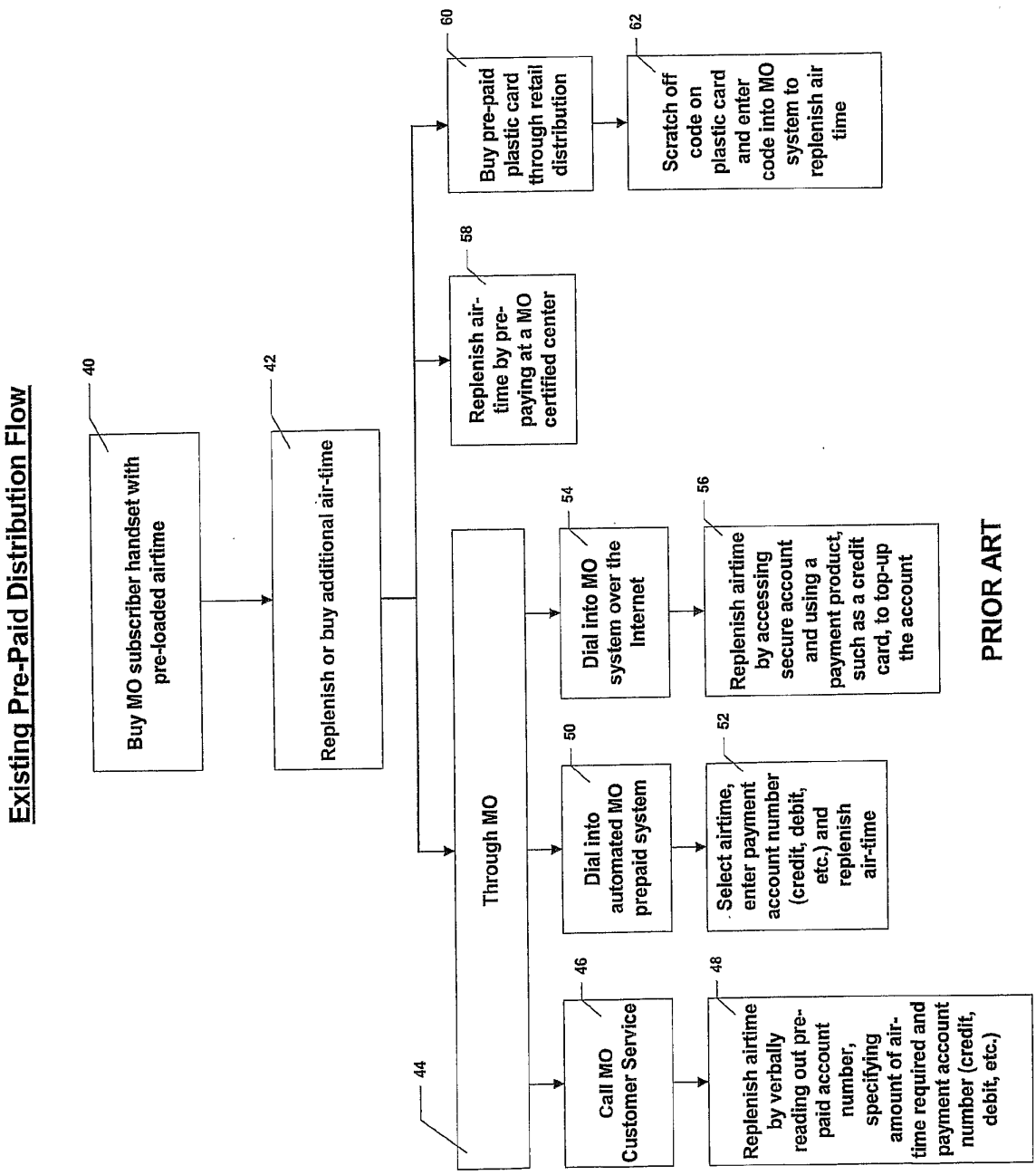
17. The method of claim 12, wherein the step of creating a virtual card comprises creating a plurality of virtual cards and the step of downloading the virtual card to a retailer electronic transaction device comprises downloading batches of virtual transaction cards to the retailer electronic transaction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

APPL-1002
APPLE INC. / Page 148 of 1892



PRIOR ART

Figure 1



PRIOR ART

Figure 2

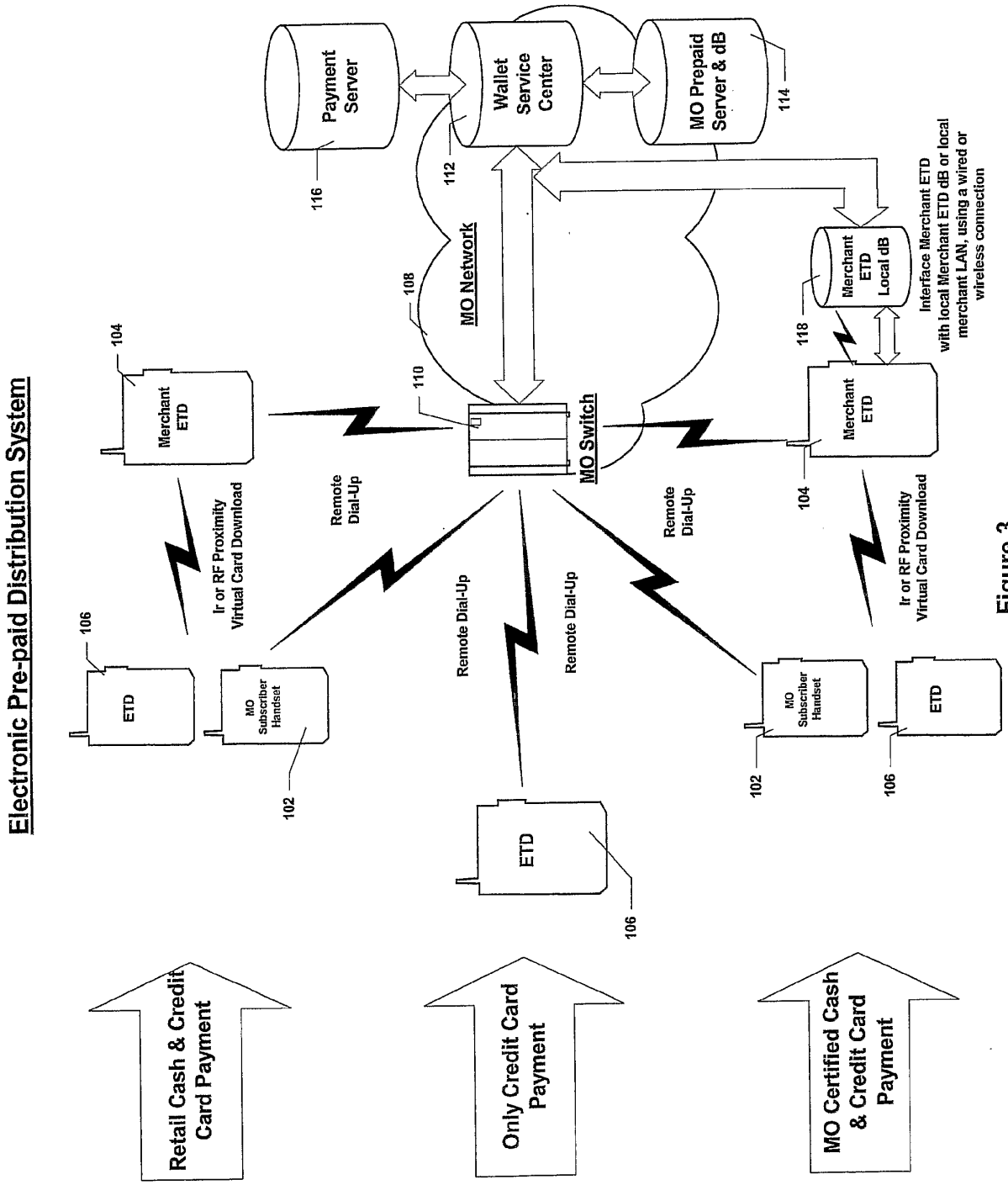

Electronic Pre-paid Distribution System
Payment Server
Wallet Service Center
MO Prepaid Server & dB
116
112
114
MO Network
108
MO Switch
110
Merchant ETD
Local dB
118
Interface Merchant ETD with local Merchant ETD dB or local merchant LAN, using a wired or wireless connection
104
Merchant ETD
Ir or RF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

Figure 3

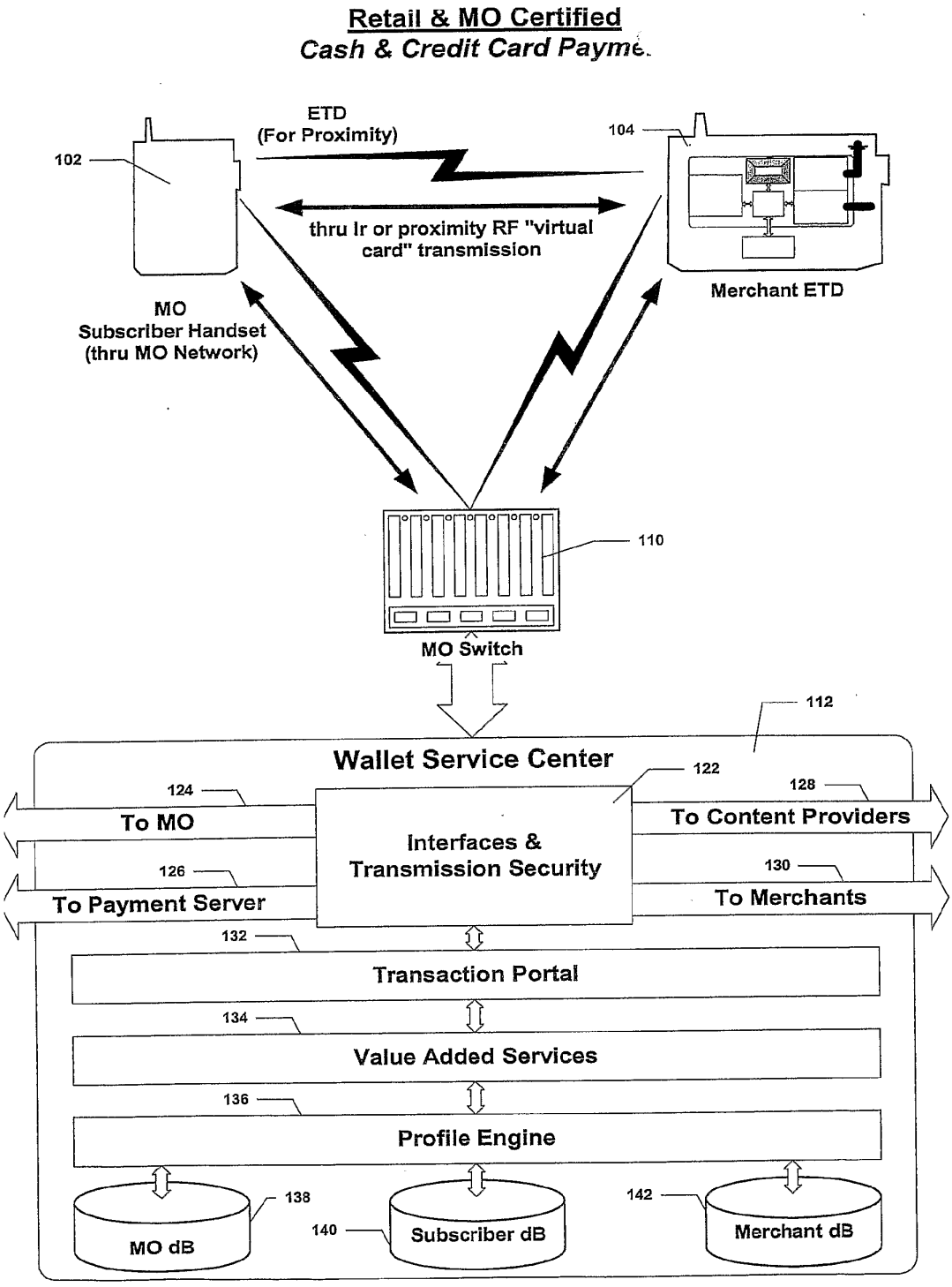

Retail & MO Certified
Cash & Credit Card Payme
ETD
(For Proximity)
102
104
thru Ir or proximity RF "virtual card" transmission
MO
Subscriber Handset
(thru MO Network)
Merchant ETD
110
MO Switch
112
Wallet Service Center
122
124
To MO
128
To Content Providers
Interfaces &
Transmission Security
126
To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

Figure 4

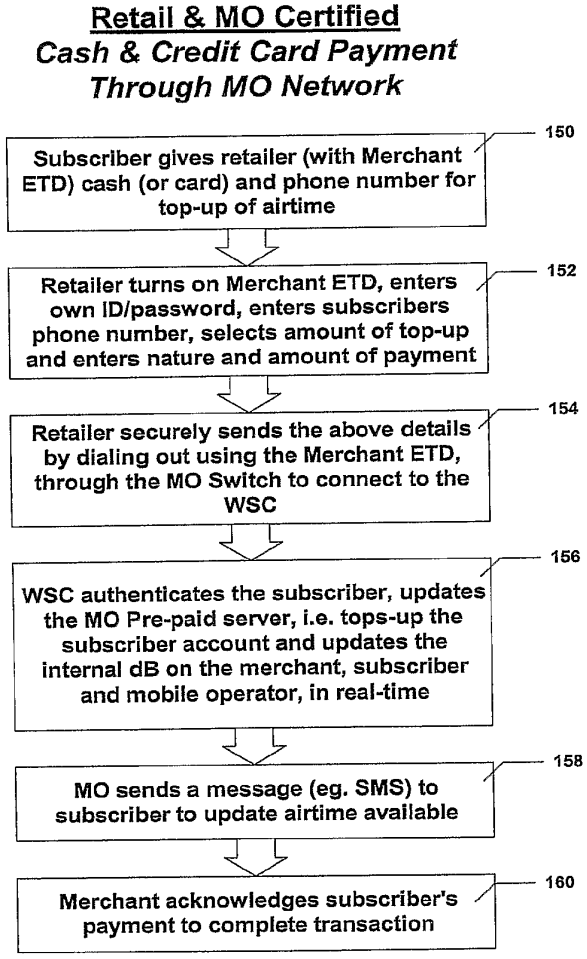

Retail & MO Certified
Cash & Credit Card Payment
Through MO Network
Subscriber gives retailer (with Merchant ETD) cash (or card) and phone number for top-up of airtime
150
Retailer turns on Merchant ETD, enters own ID/password, enters subscribers phone number, selects amount of top-up and enters nature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

Figure 5

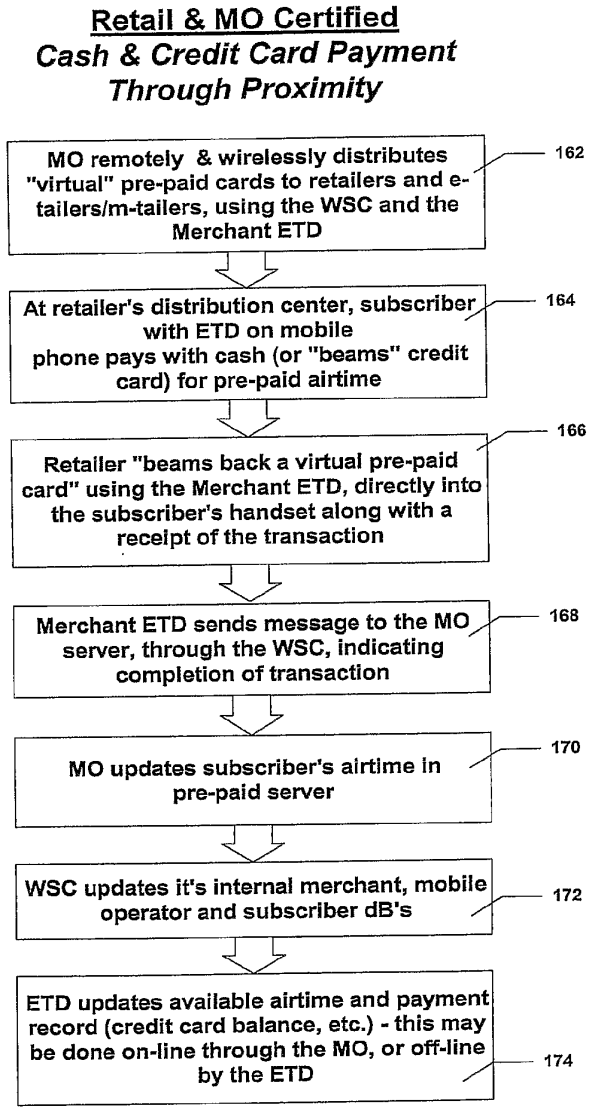

Retail & MO Certified
Cash & Credit Card Payment
Through Proximity
MO remotely & wirelessly distributes "virtual" pre-paid cards to retailers and e-tailers/m-tailers, using the WSC and the Merchant ETD
162
At retailer's distribution center, subscriber with ETD on mobile phone pays with cash (or "beams"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

Figure 6

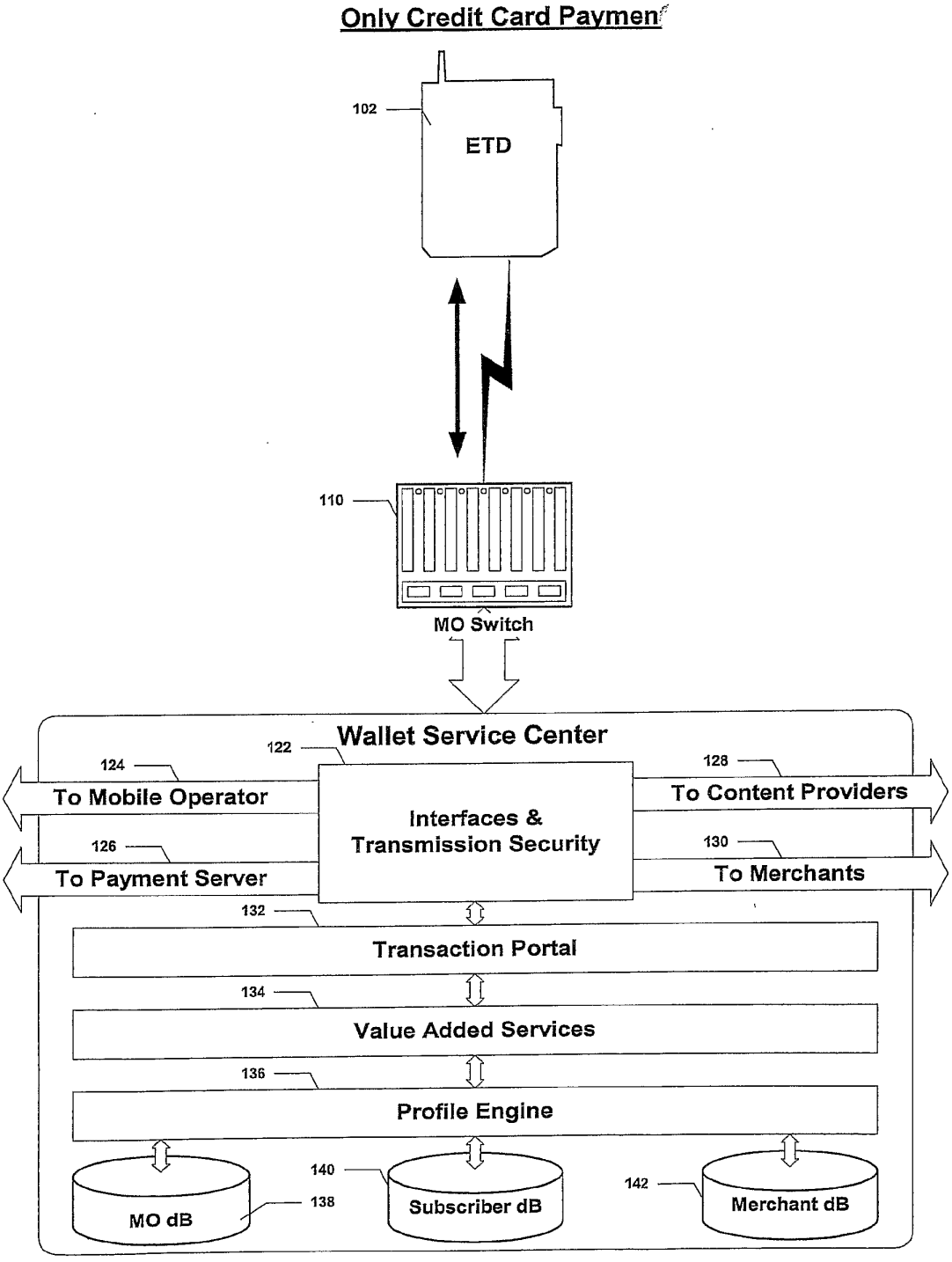

Only Credit Card Paymen
102
ETD
110
MO Switch
Wallet Service Center
122
124
To Mobile Operator
126
To Payment Server
Interfaces &
Transmission Security
128
To Content Providers
130
To Merchants
132
Transaction Portal
134
Value Added Services
136
Profile Engine
140
Subscriber dB
142
Merchant dB
138
MO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

Figure 7

Only Credit Card Payment - Setup Sequence Flow Chart

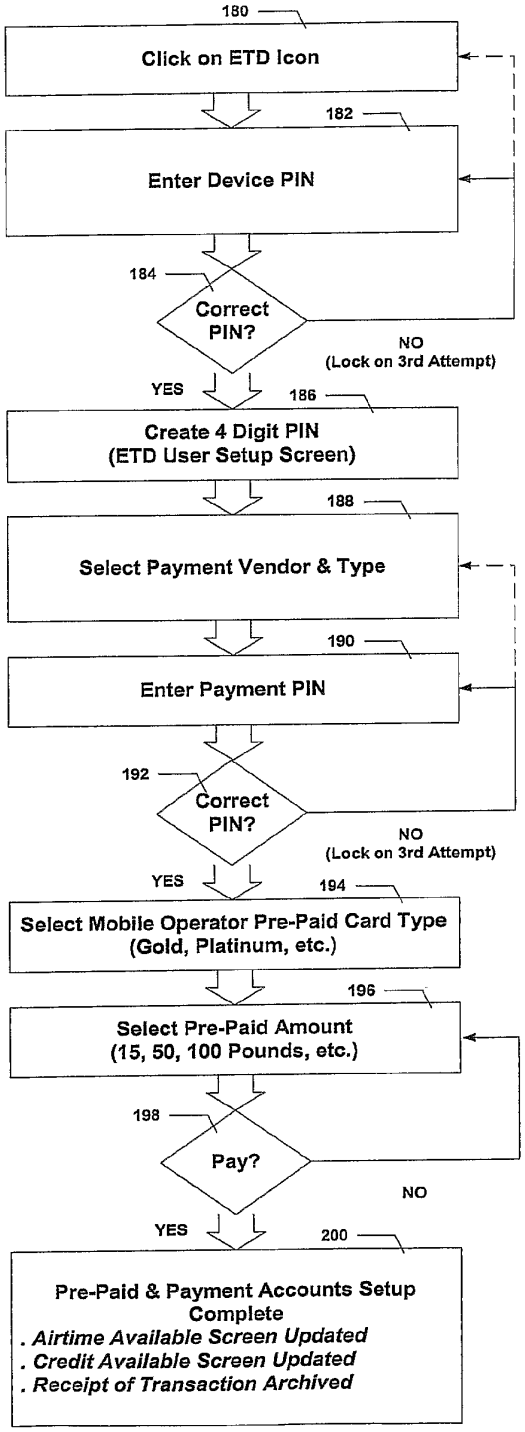


Figure 8

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

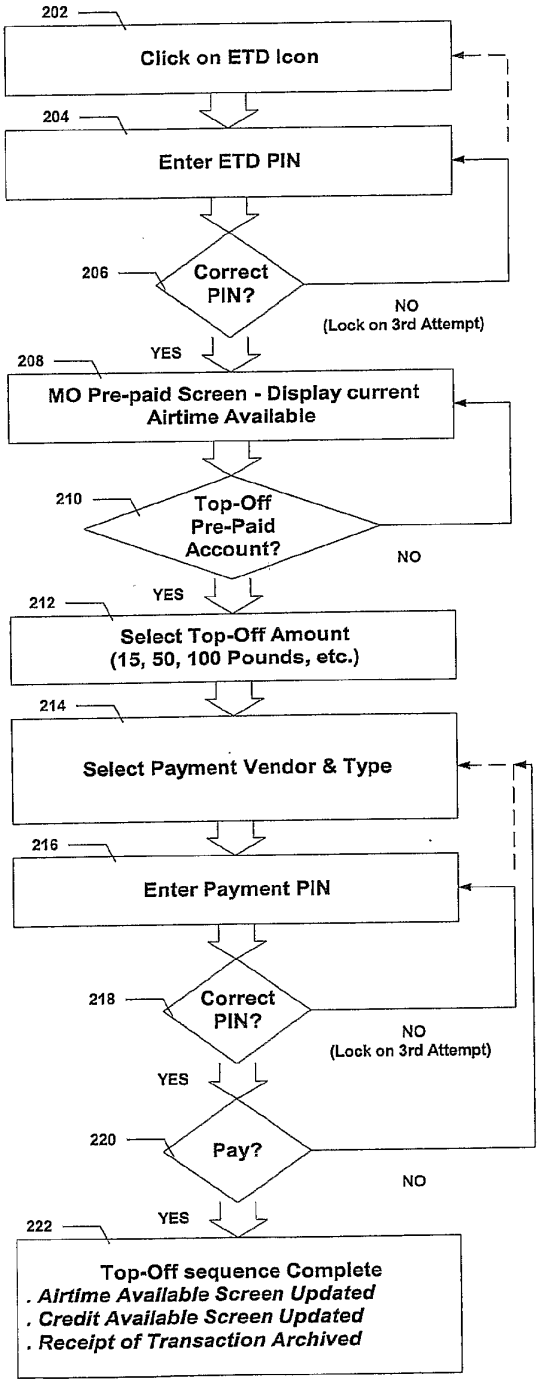


Figure 9

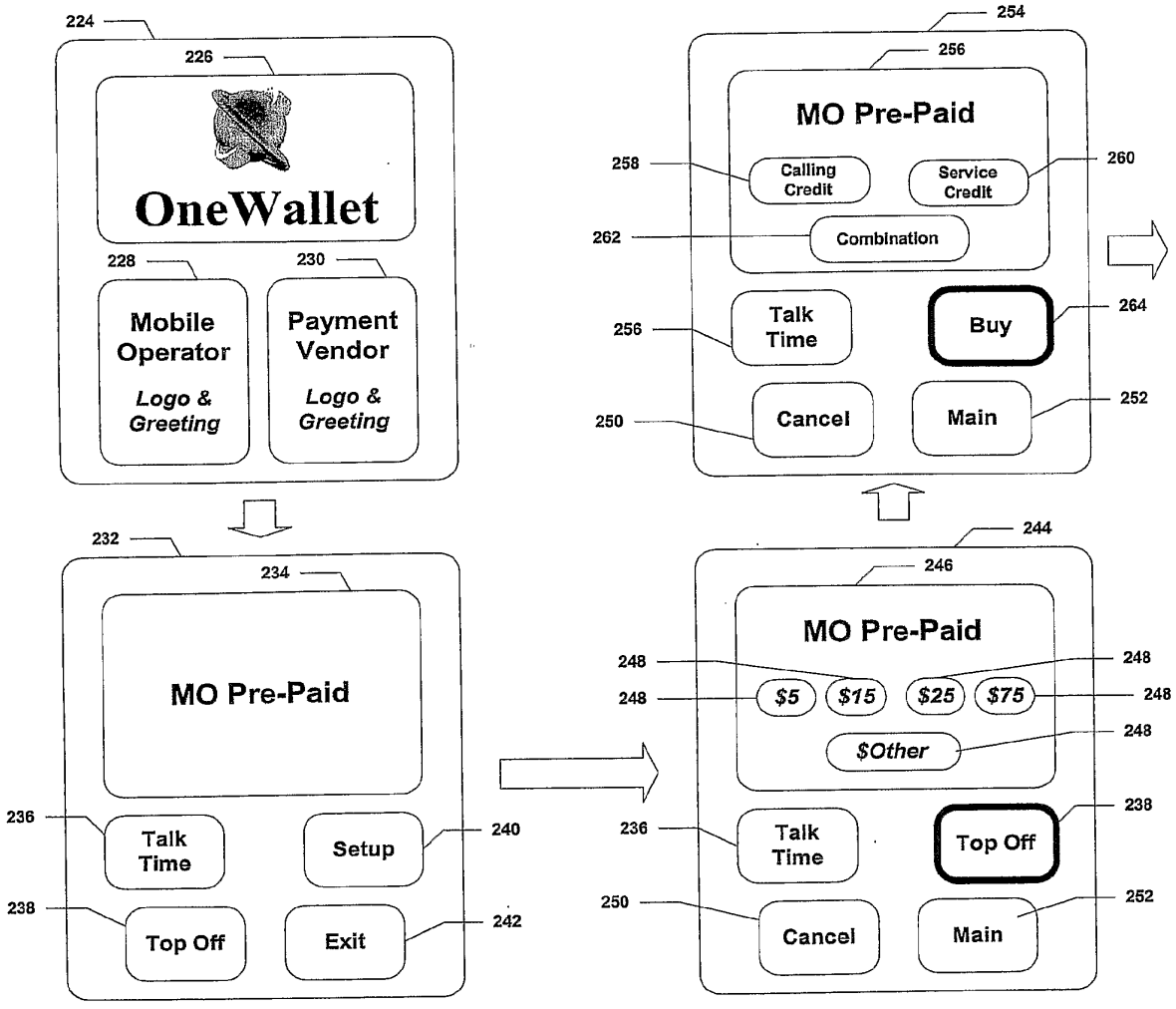

Only Credit Card Payment
Sample UIs
224
226
OneWallet
228
Mobile Operator
Logo & Greeting
230
Payment Vendor
Logo & Greeting
232
234
MO Pre-Paid
236
Talk Time
238
Top Off
240
Setup
242
Exit
254
256
MO Pre-Paid
258
Calling Credit
260
Service Credit
262
Combination
256
Talk Time
264
Buy
250
Cancel
252
Main
244
246
MO Pre-Paid
248
$5
$15
$25
$75
$Other
236
Talk Time
238
Top Off
250
Cancel
252
Main

Figure 10

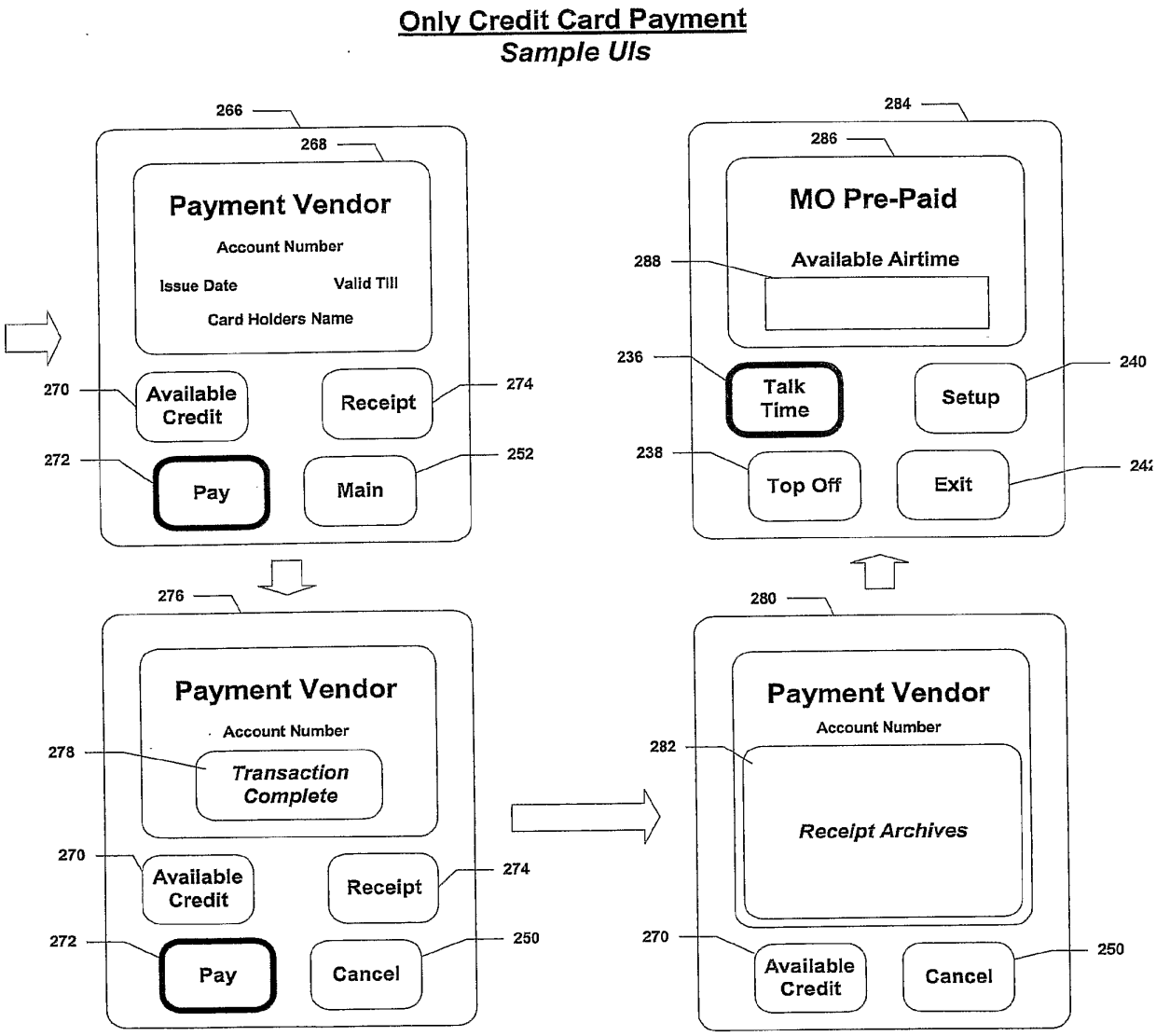

Only Credit Card Payment
Sample UIs
266
268
Payment Vendor
Account Number
Issue Date
Valid Till
Card Holders Name
270
Available Credit
Receipt
274
272
Pay
Main
252
284
286
MO Pre-Paid
288
Available Airtime
236
Talk Time
Setup
240
238
Top Off
Exit
276
Payment Vendor
Account Number
278
Transaction Complete
270
Available Credit
Receipt
274
272
Pay
Cancel
250
280
Payment Vendor
Account Number
282
Receipt Archives
270
Available Credit
Cancel
250

Figure 11

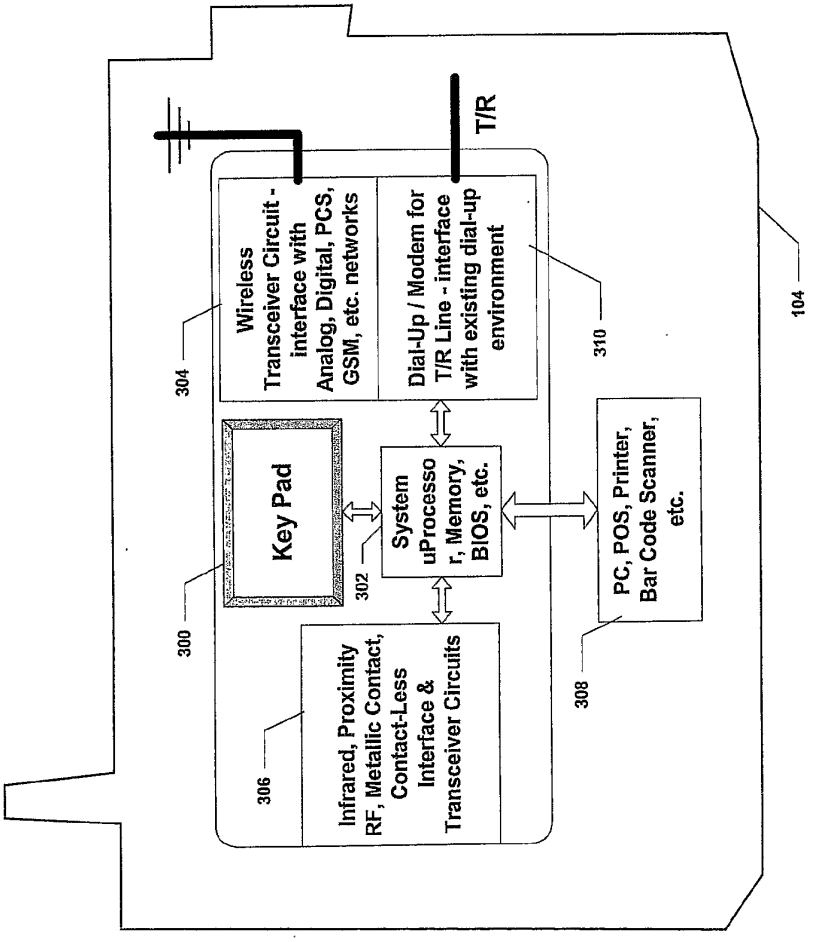

Merchant ETD Architecture
Wireless Transceiver Circuit - interface with Analog, Digital, PCS, GSM, etc. networks
Dial-Up / Modem for T/R Line - interface with existing dial-up environment
T/R
Key Pad
System uProcesso r, Memory, BIOS, etc.
PC, POS, Printer, Bar Code Scanner, etc.
Infrared, Proximity RF,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

Figure 12

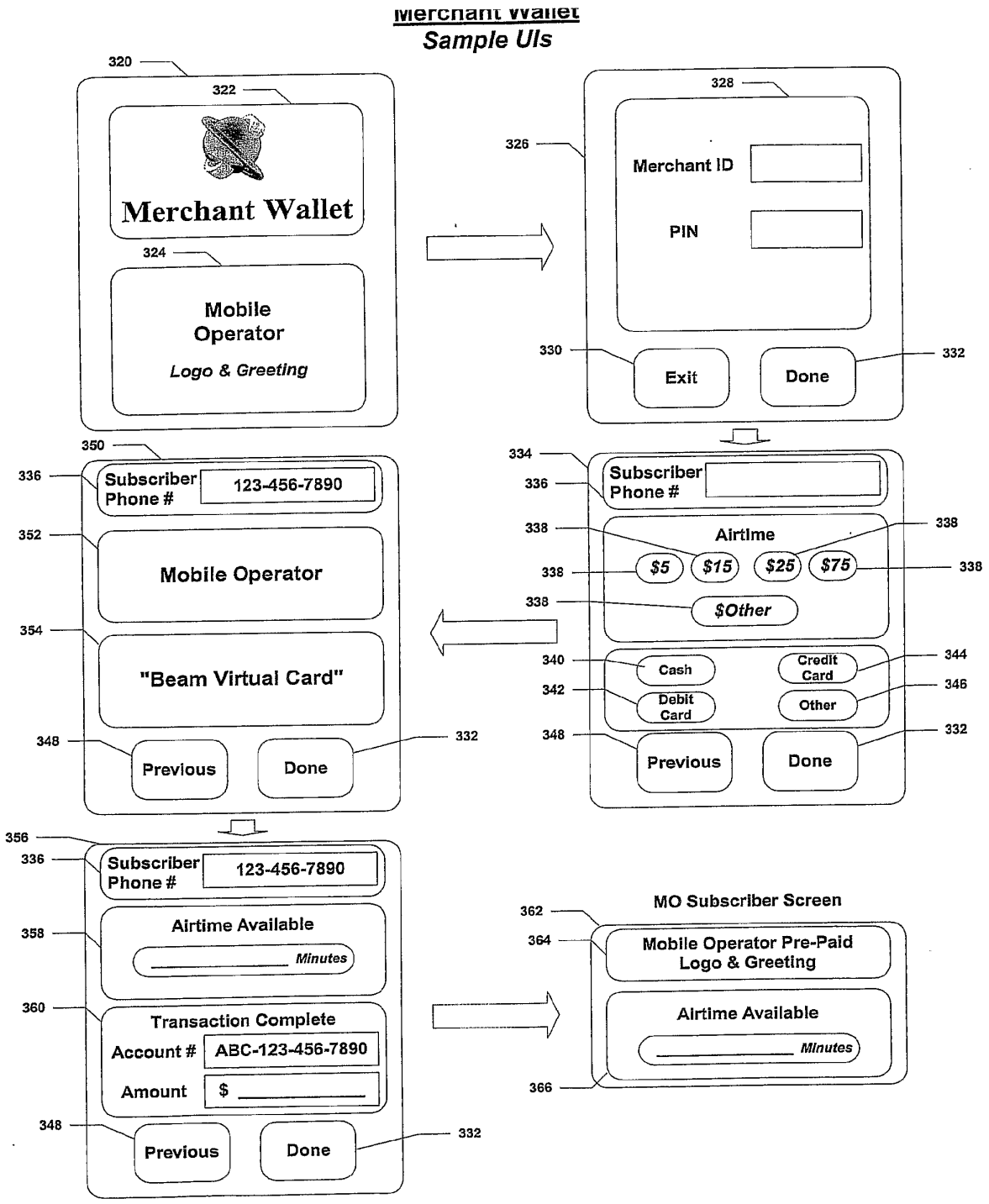

Merchant Wallet
Sample UIs
320
322
Merchant Wallet
324
Mobile Operator
Logo & Greeting
326
328
Merchant ID
PIN
330
Exit
Done
332
334
336
Subscriber Phone #
338
Airtime
$5
$15
$25
$75
$Other
340
Cash
Credit Card
342
Debit Card
Other
344
346
348
Previous
Done
350
352
Mobile Operator
354
"Beam Virtual Card"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

Figure 13

Wallet Service Center
Value Added Services

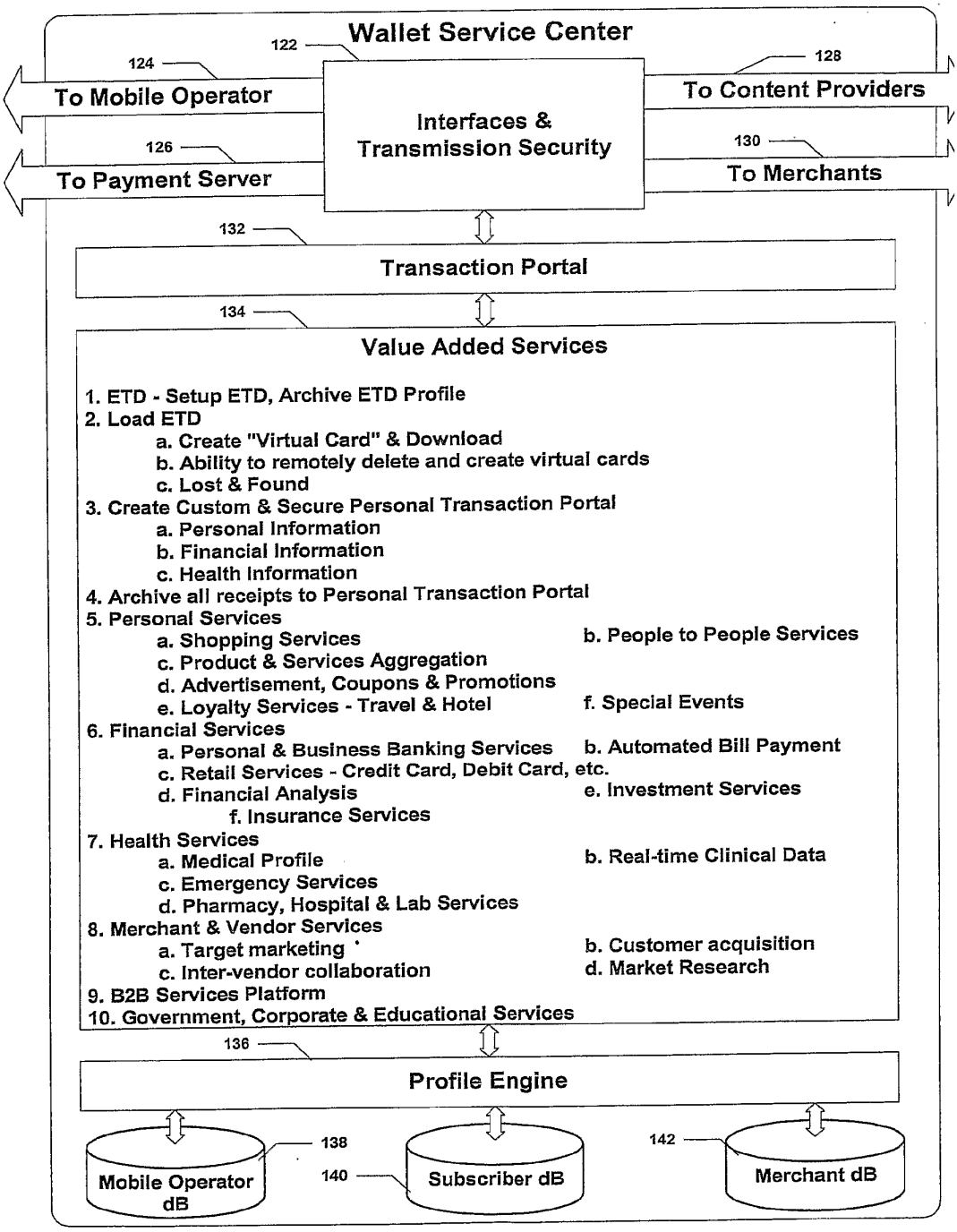
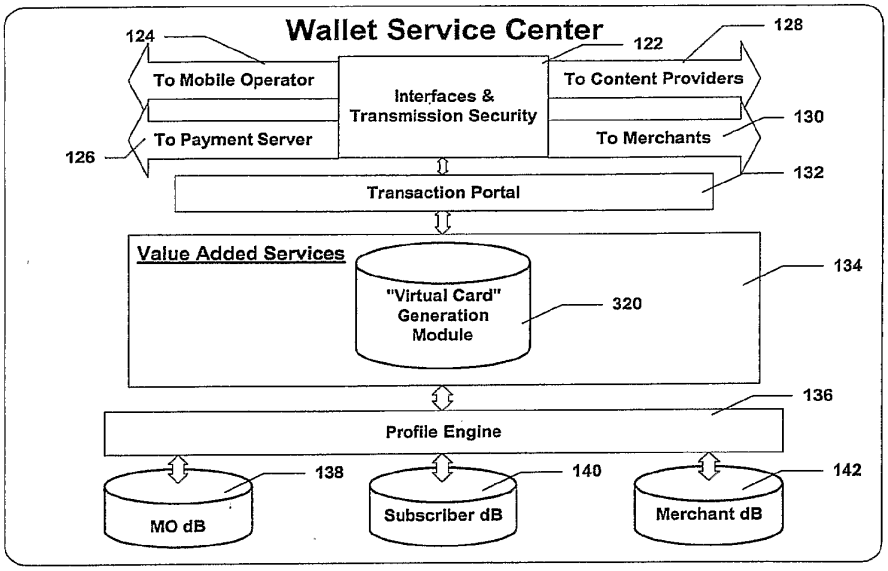
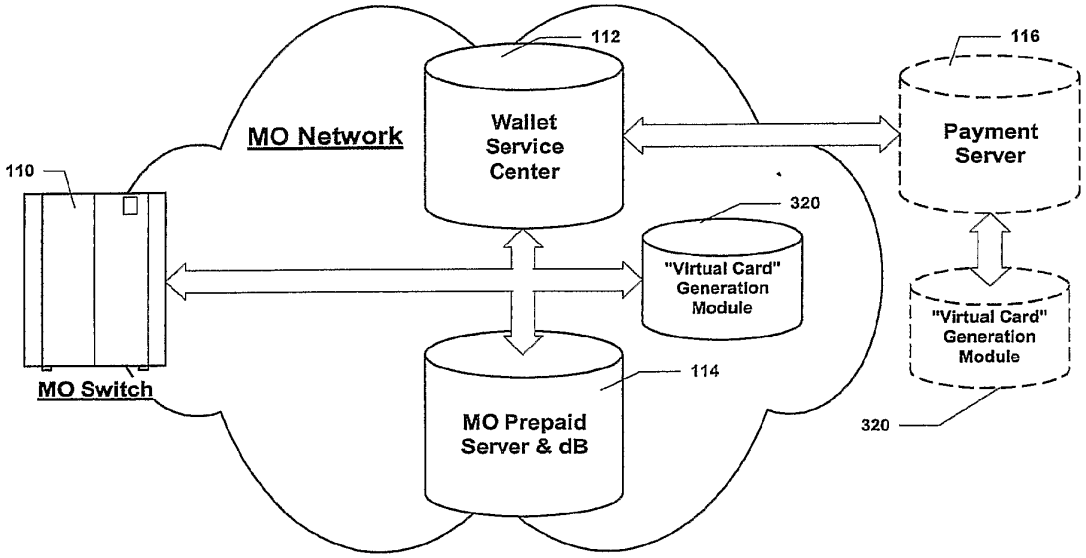


Figure 14

"Virtual Card" Generation & Download



A



B

Figure 15

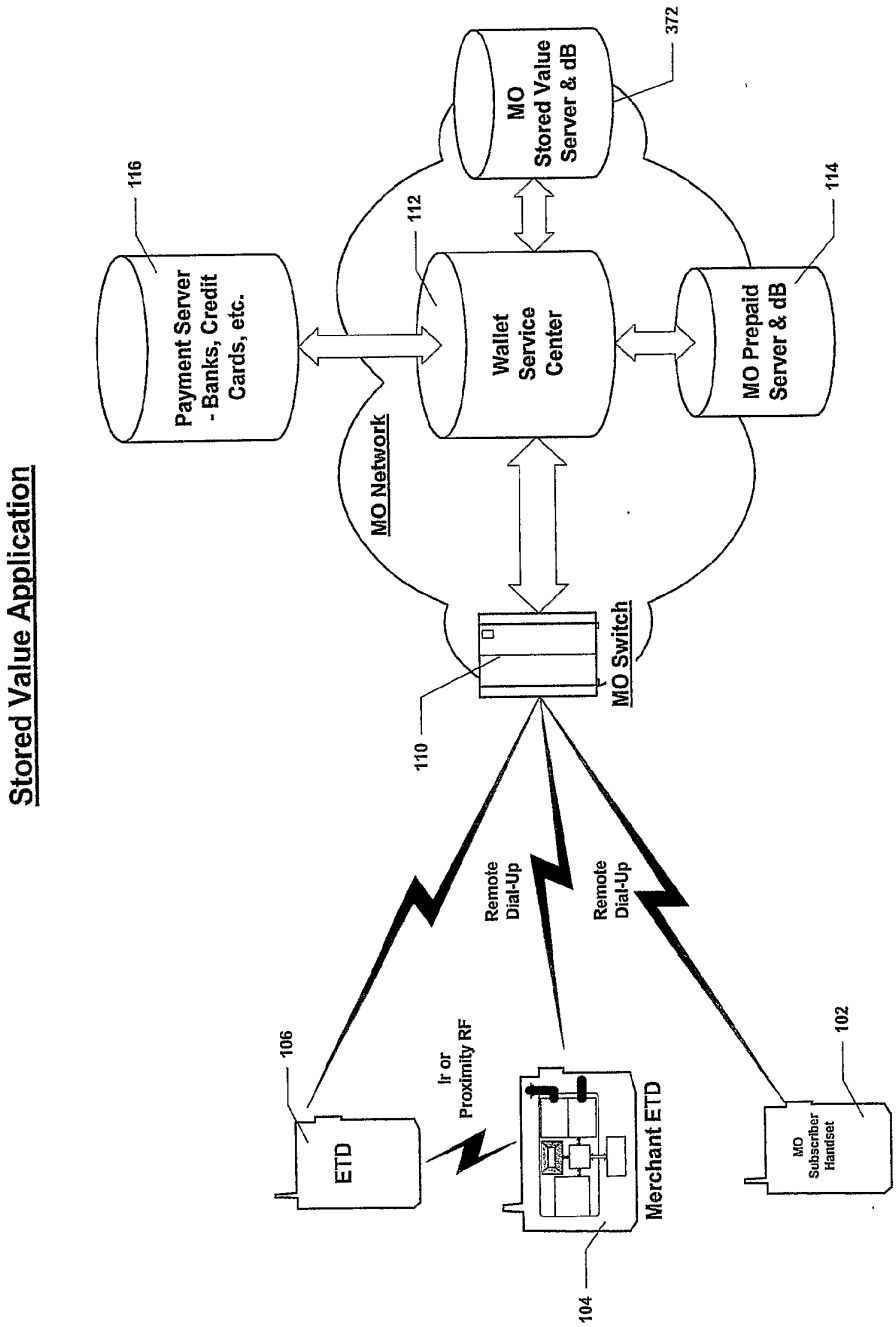

Stored Value Application
MO Stored Value Server & dB
372
116
Payment Server - Banks, Credit Cards, etc.
112
Wallet Service Center
114
MO Prepaid Server & dB
MO Network
MO Switch
110
Remote Dial-Up
Remote Dial-Up
106
Ir or Proximity RF
ETD
Merchant ETD
104
102
MO Subscriber Handset

Figure 16

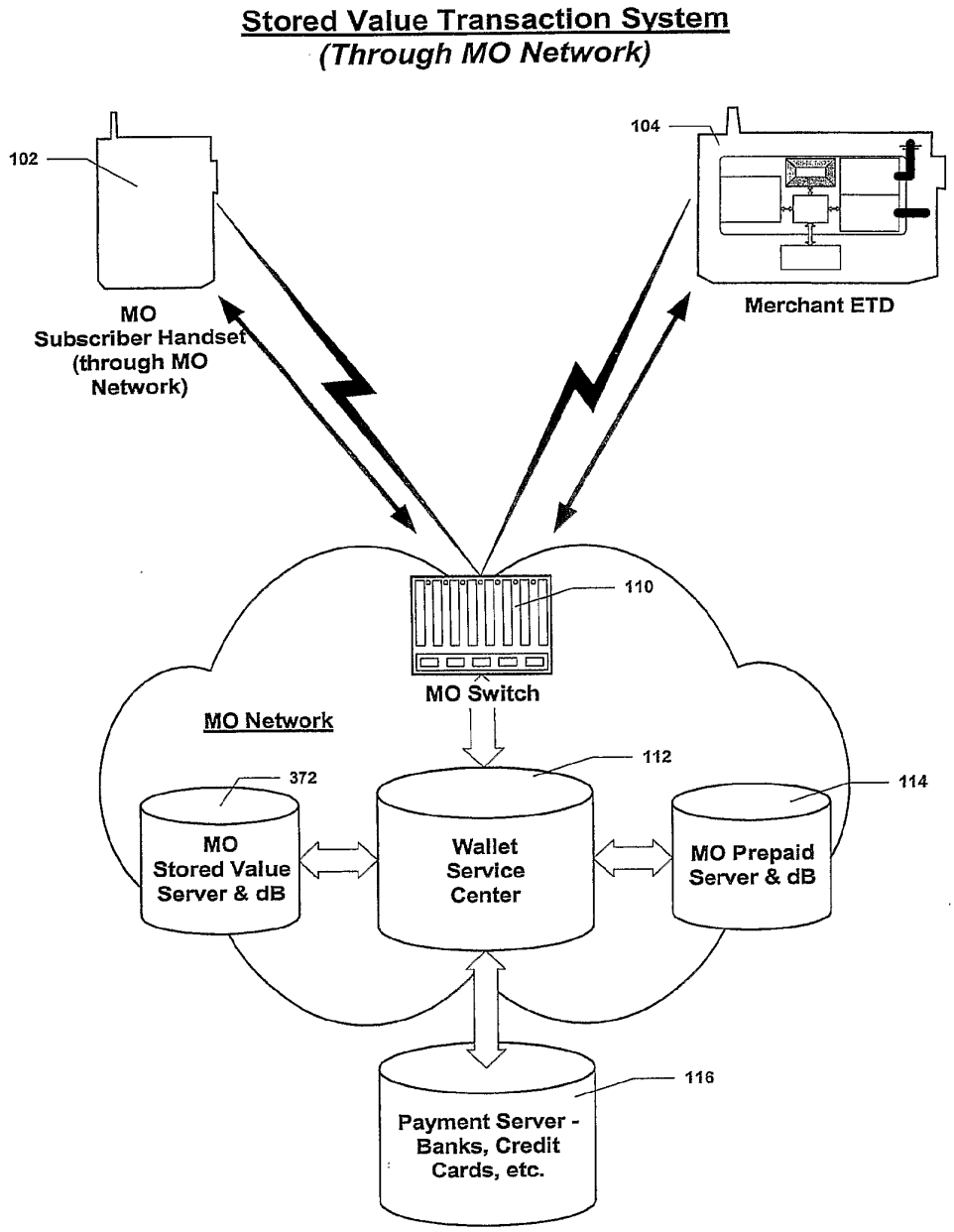

Stored Value Transaction System
(Through MO Network)
102
MO
Subscriber Handset
(through MO
Network)
104
Merchant ETD
110
MO Switch
MO Network
372
MO
Stored Value
Server & dB
112
Wallet
Service
Center
114
MO Prepaid
Server & dB
116
Payment Server -
Banks, Credit
Cards, etc.

Figure 17

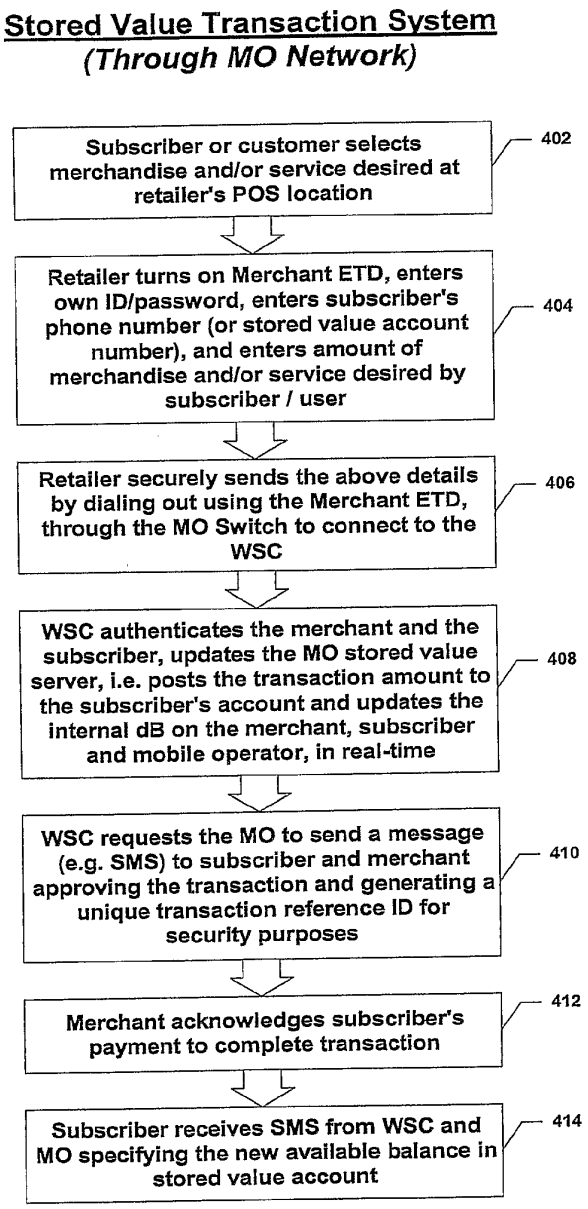

Stored Value Transaction System
(Through MO Network)
Subscriber or customer selects merchandise and/or service desired at retailer's POS location
402
Retailer turns on Merchant ETD, enters own ID/password, enters subscriber's phone number (or stored value account number), and enters amount of merchandise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

Figure 18

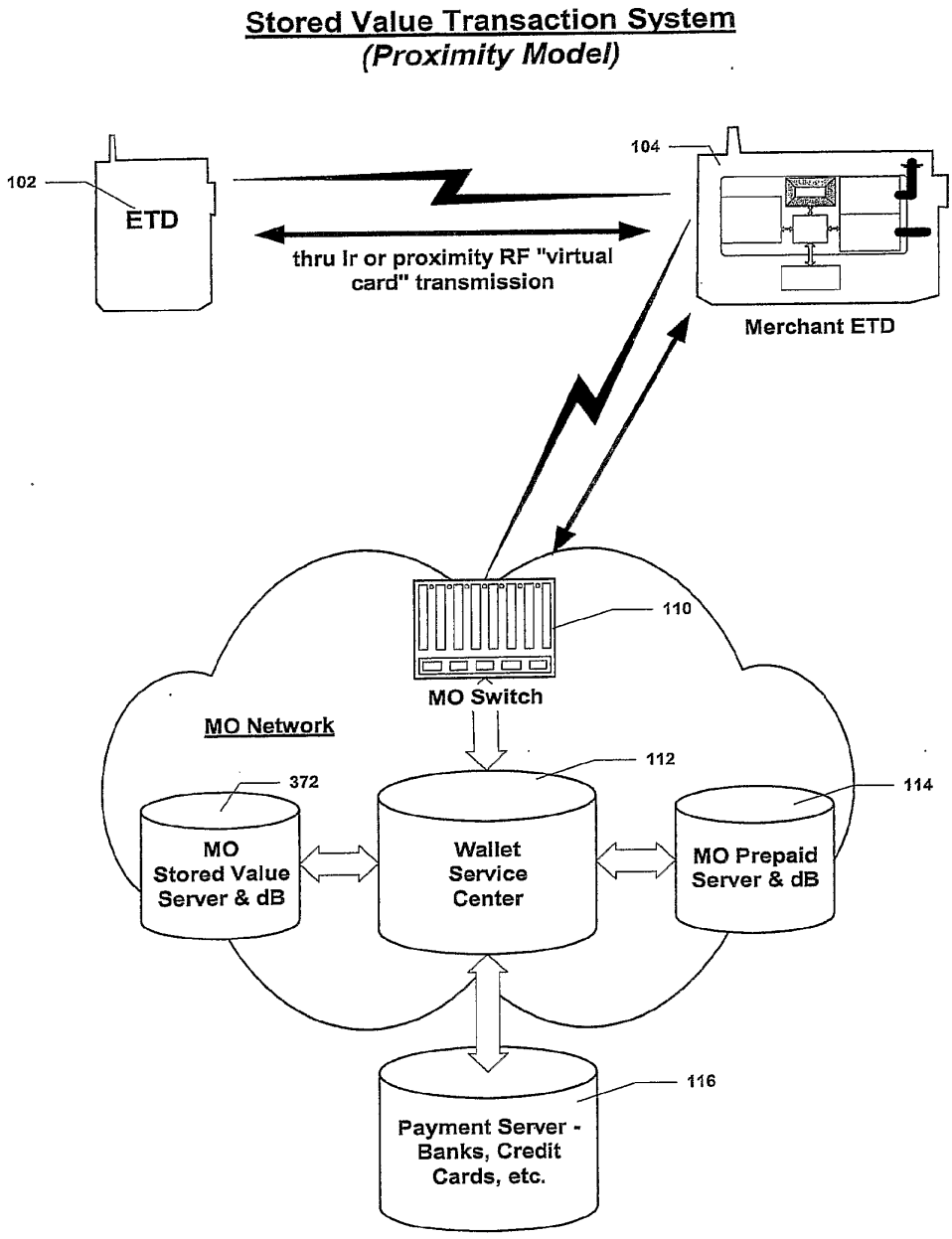

Stored Value Transaction System
(Proximity Model)
102
ETD
104
thru Ir or proximity RF "virtual card" transmission
Merchant ETD
110
MO Switch
MO Network
112
372
114
MO Stored Value Server & dB
Wallet Service Center
MO Prepaid Server & dB
116
Payment Server - Banks, Credit Cards, etc.

Figure 19

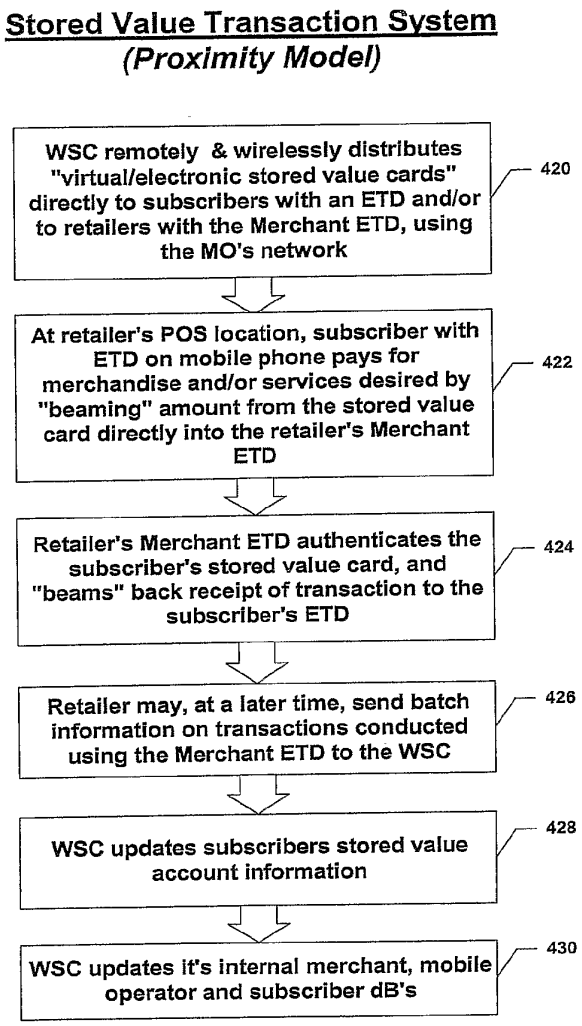

Stored Value Transaction System
(Proximity Model)
WSC remotely & wirelessly distributes "virtual/electronic stored value cards" directly to subscribers with an ETD and/or to retailers with the Merchant ETD, using the MO's network
420
At retailer's POS location, subscriber with ETD on mobile phone pays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

Figure 20

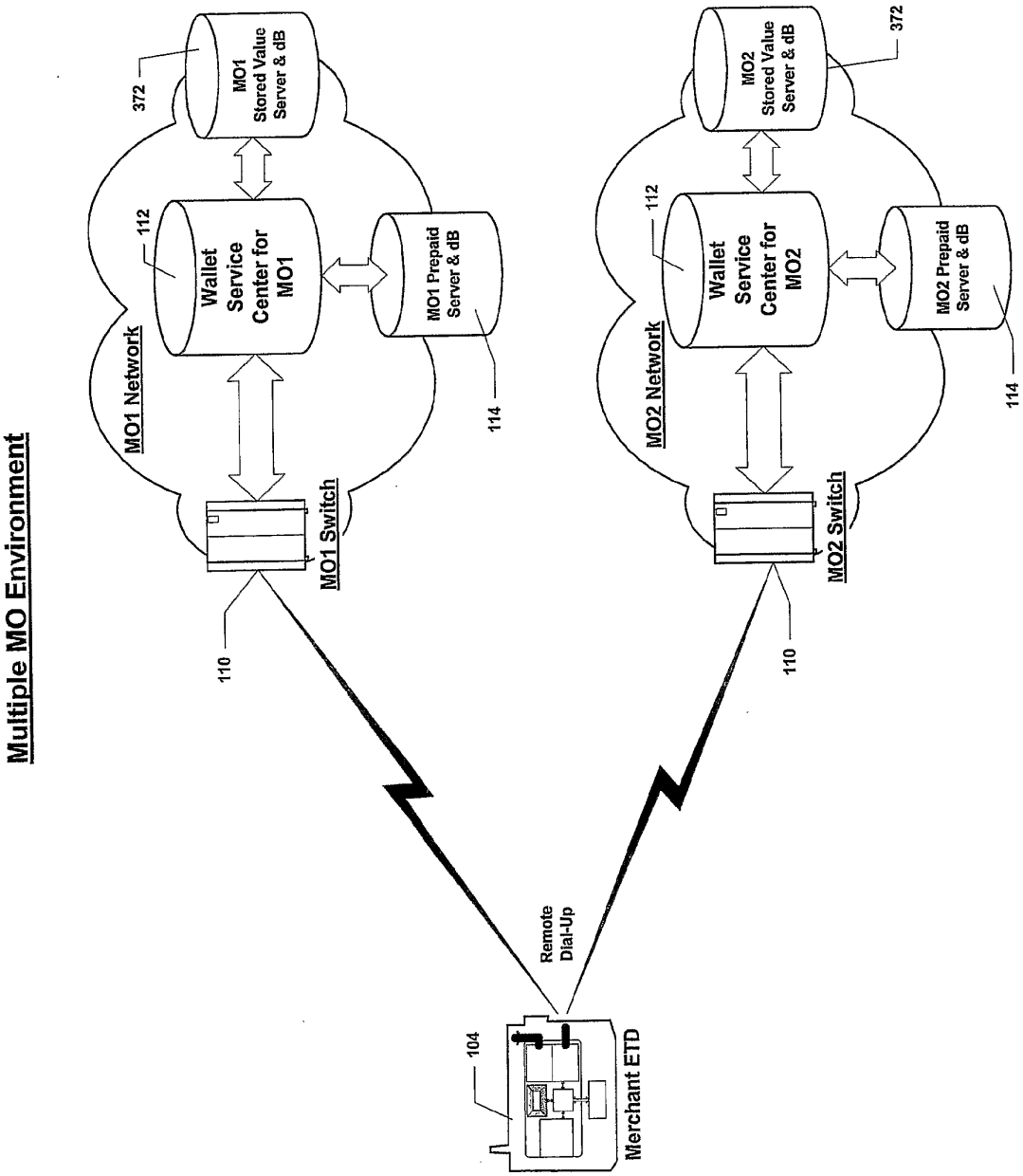

Multiple MO Environment
MO1 Network
MO1 Stored Value Server & dB
372
Wallet Service Center for MO1
112
MO1 Prepaid Server & dB
114
MO1 Switch
110
MO2 Network
MO2 Stored Value Server & dB
372
Wallet Service Center for MO2
112
MO2 Prepaid Server & dB
114
MO2 Switch
110
Remote Dial-Up
104
Merchant ETD

Figure 21

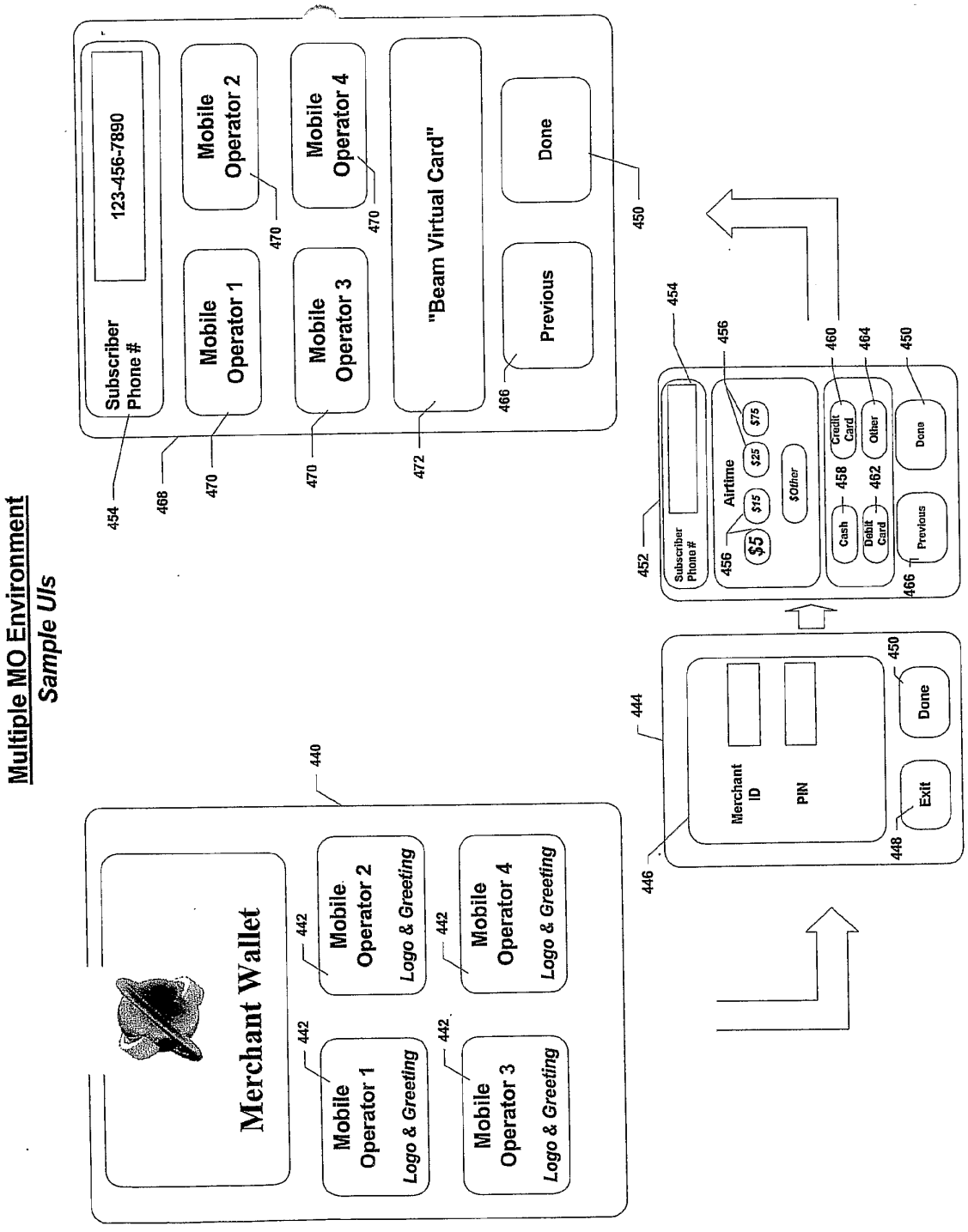

Multiple MO Environment
Sample UIs
Merchant Wallet
Mobile Operator 1
Logo & Greeting
Mobile Operator 2
Logo & Greeting
Mobile Operator 3
Logo & Greeting
Mobile Operator 4
Logo & Greeting
Subscriber Phone #
123-456-7890
Mobile Operator 1
Mobile Operator 2
Mobile Operator 3
Mobile Operator 4
"Beam Virtual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

Figure 22

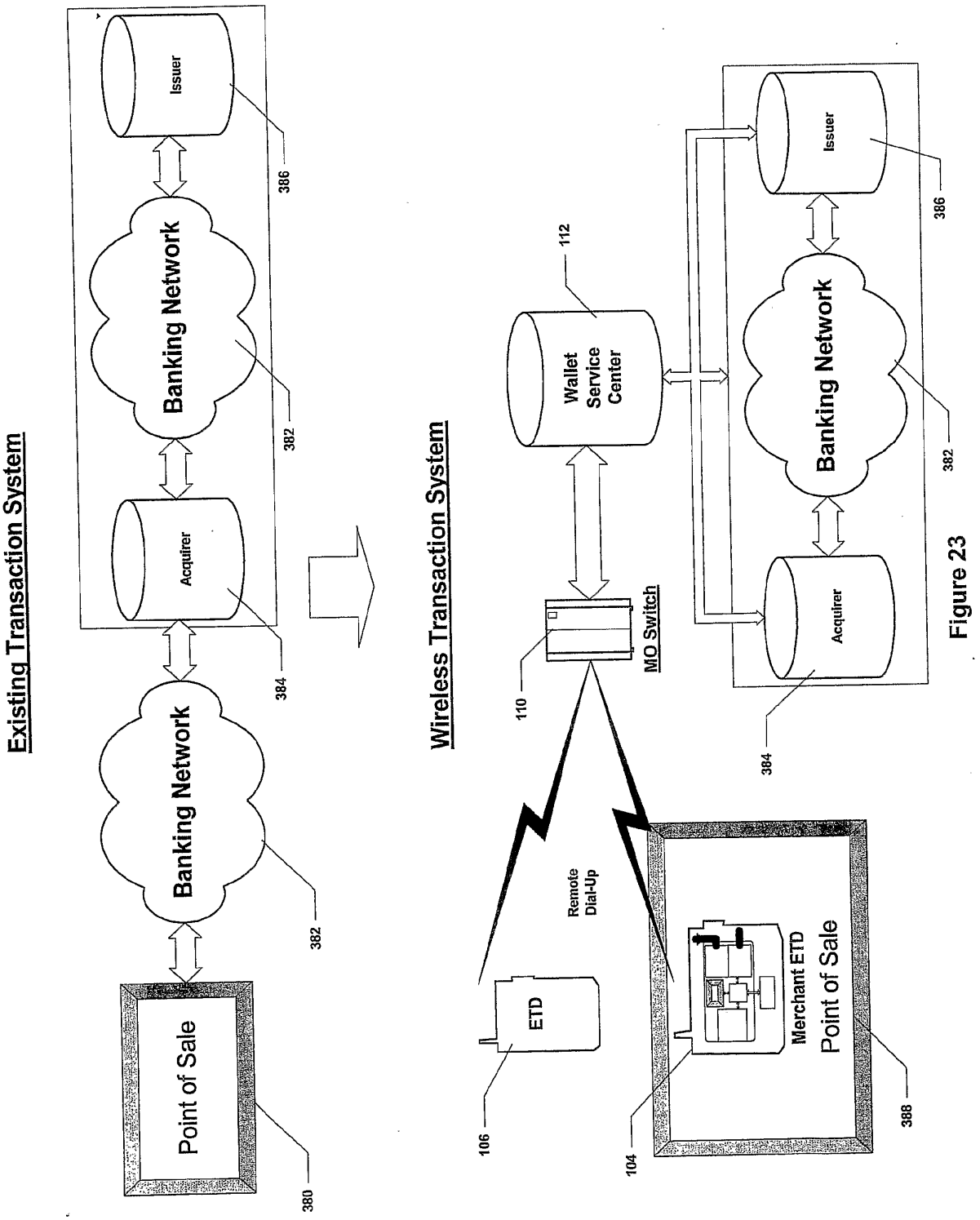

Existing Transaction System
Issuer
386
Banking Network
382
Acquirer
384
Banking Network
382
Point of Sale
380
Wireless Transaction System
112
Wallet Service Center
Issuer
386
Banking Network
382
110
MO Switch
Acquirer
384
Remote Dial-Up
ETD
106
Merchant ETD
Point of Sale
104
388

Figure 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/23899

A. CLASSIFICATION OF SUBJECT MATTER

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

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

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

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

EAST, search terms: pre-paid, virtual card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

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

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

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

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

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

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

(19) World Intellectual Property Organization
International Bureau

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

PCT

(10) International Publication Number
WO 2004/010393 A1

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

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

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

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventor; and

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

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

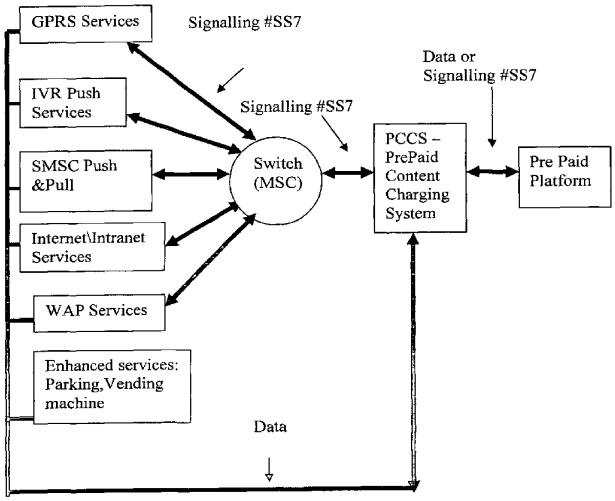
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

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

Published:
— *with international search report*

[Continued on next page]

(54) Title: PREPAID CHARGING SYSTEM AND METHOD



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

WO 2004/010393 A1

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

PREPAID CHARGING SYSTEM AND METHOD

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

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

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

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

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

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

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

Summary of the Invention

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

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

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

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

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

Brief Description of the Drawings

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

Detailed Description of the Invention in Respect of a Preferred Embodiment

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

APPL-1002
APPLE INC. / Page 178 of 1892

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Claims:

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

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

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

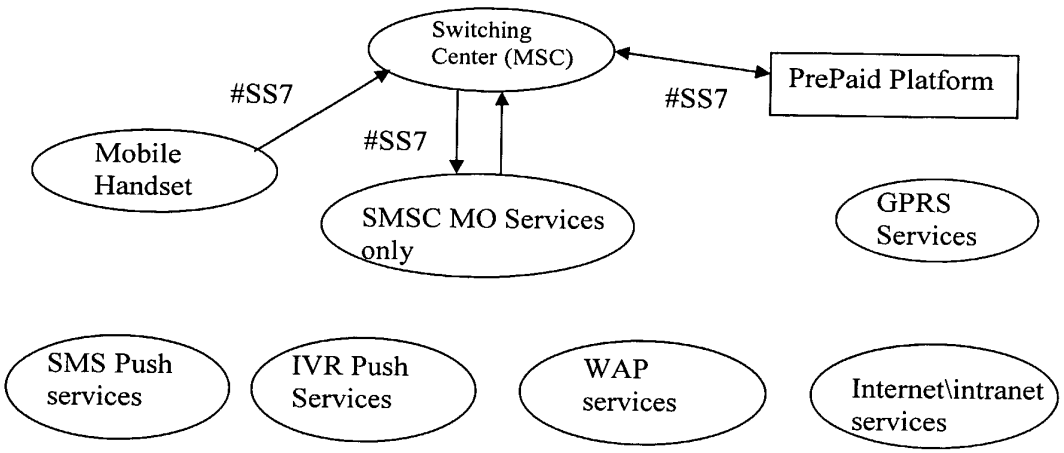

Switching Center (MSC)
PrePaid Platform
#SS7
#SS7
#SS7
Mobile Handset
SMSC MO Services only
GPRS Services
SMS Push services
IVR Push Services
WAP services
Internet\intranet services

Fig. 1

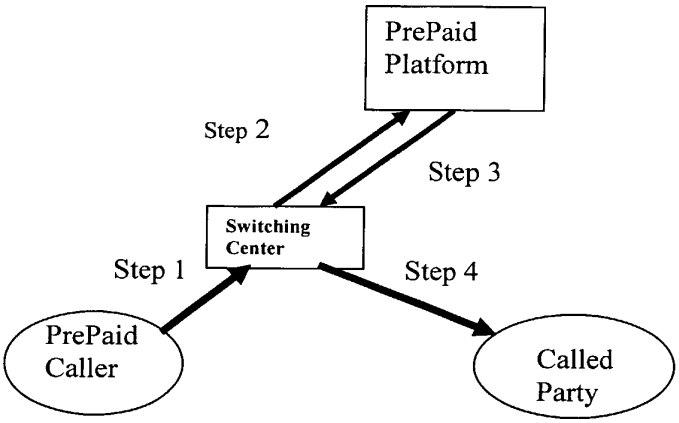

PrePaid
Platform
Step 2
Step 3
Switching
Center
Step 1
Step 4
PrePaid
Caller
Called
Party

Fig. 2

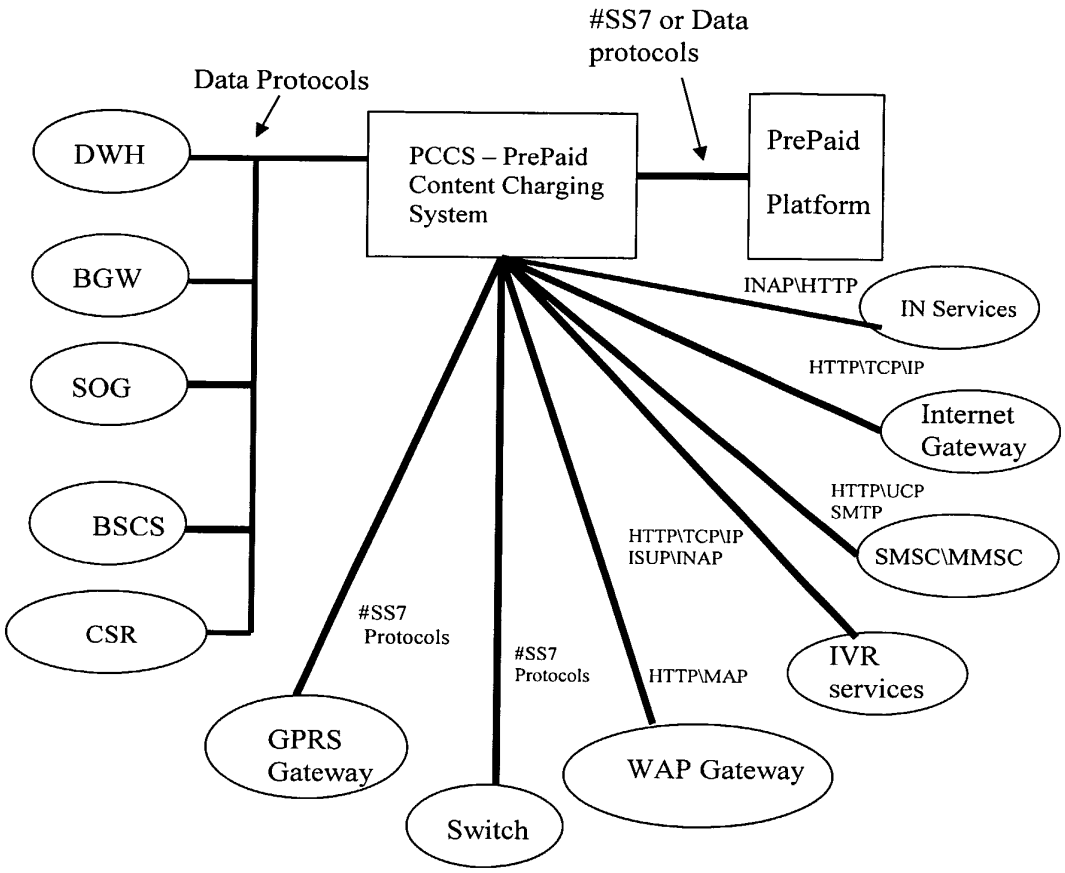

#SS7 or Data protocols
Data Protocols
DWH
BGW
SOG
BSCS
CSR
PCCS – PrePaid Content Charging System
PrePaid Platform
INAP\HTTP
IN Services
HTTP\TCP\IP
Internet Gateway
HTTP\UCP SMTP
SMSC\MMSC
HTTP\TCP\IP ISUP\INAP
IVR services
#SS7 Protocols
#SS7 Protocols
HTTP\MAP
GPRS Gateway
Switch
WAP Gateway

Fig. 3

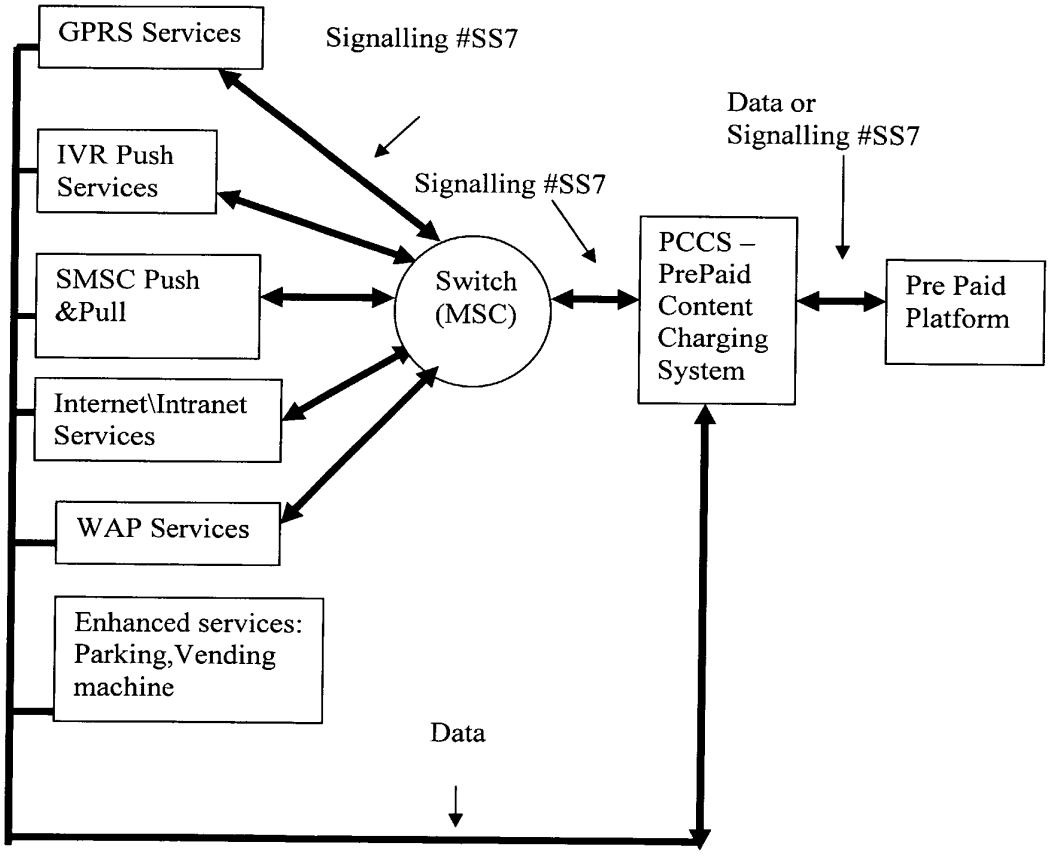

GPRS Services
Signalling #SS7
Data or
Signalling #SS7
IVR Push
Services
Signalling #SS7
SMSC Push
&Pull
Switch
(MSC)
PCCS –
PrePaid
Content
Charging
System
Pre Paid
Platform
Internet\Intranet
Services
WAP Services
Enhanced services:
Parking,Vending
machine
Data

Fig. 4

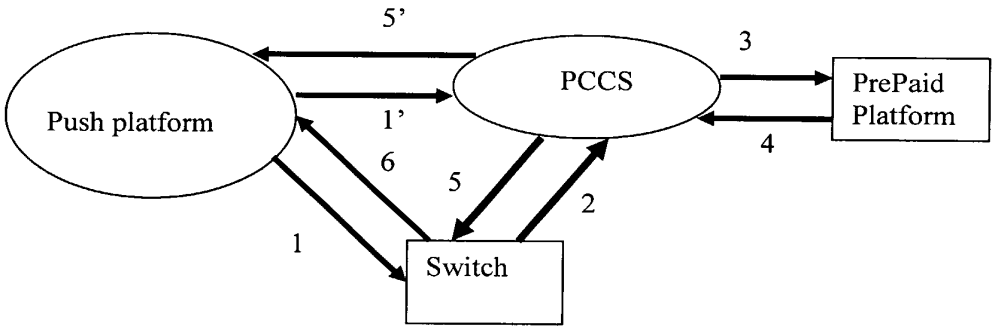


Fig. 5

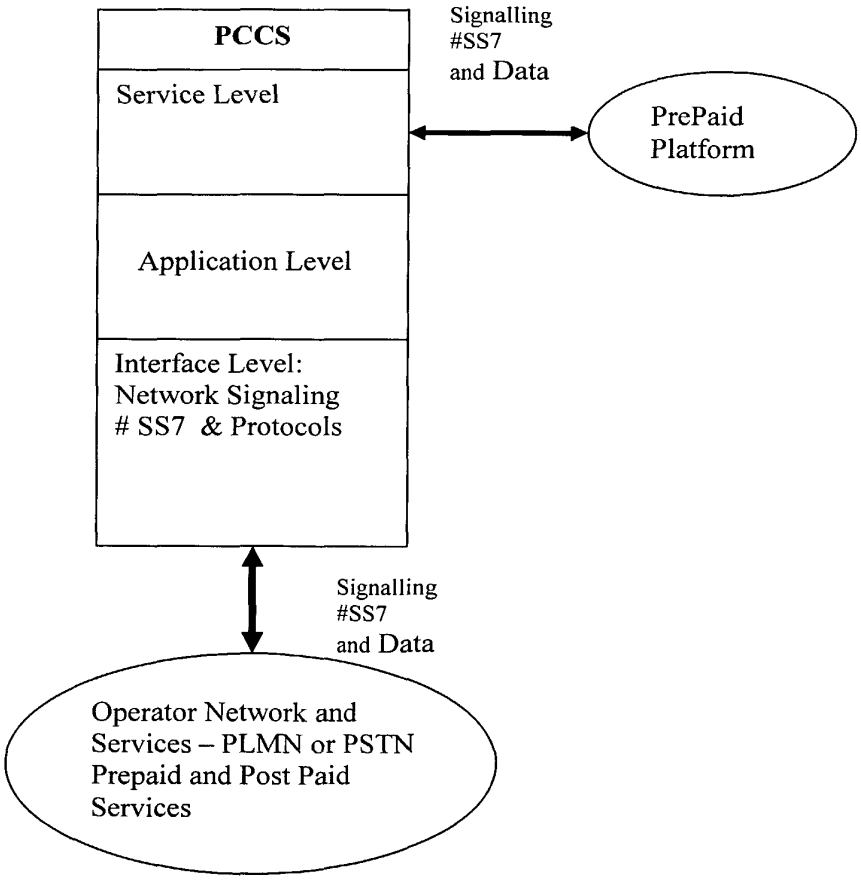

PCCS
Service Level
Application Level
Interface Level:
Network Signaling
SS7 & Protocols
Signalling
#SS7
and Data
PrePaid
Platform
Signalling
#SS7
and Data
Operator Network and
Services – PLMN or PSTN
Prepaid and Post Paid
Services

Fig. 6

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

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

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

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

-/--

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

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

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

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

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

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

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

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00601

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

(11) Application No. AU 2007312879 A1

(19) AUSTRALIAN PATENT OFFICE

(54) Title
An interactive system and process

(51)[6] International Patent Classification(s)
H04M 3/493 (2006.01)
H04W 4/14 (2009.01)
H04M 3/493 20060101AFI2008042
4BHAU H04W 4/14 20090101ALI2009052
9BHAU PCT/AU2007/001599

(21) Application No: 2007312879

(22) Application Date: 2007.10.19

(87) WIPO No: WO08/046161

(30) Priority Data

(31) Number	(32) Date	(33) Country
2006905829	2006.10.19	AU

(43) Publication Date : 2008.04.24

(71) Applicant(s)
Fruitful Technologies Pty Ltd

(72) Inventor(s)
Ngo, Duc Anh

(74) Agent/Attorney
Blake Dawson Patent Attorneys, Level 36, Groevenor Place 225 George Street, Sydney, NSW, 2000

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [—/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

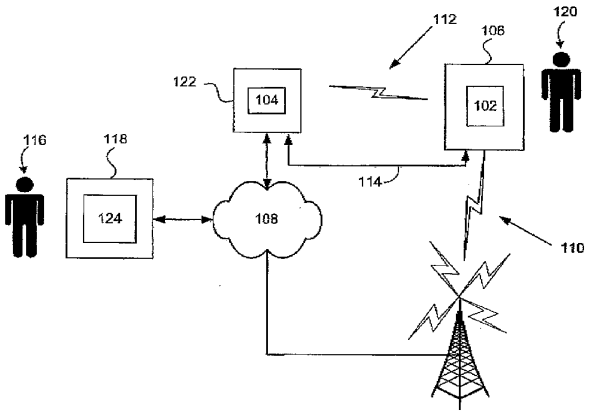
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(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, ME, 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).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;

(ii) interprets these instructions;

(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and

(iv) sends responses back to the gateway 104 or other computer system or device.

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
# START
BRANCH_TO     "serv" "Service Request"
ITEM          "Water" WATER
ITEM          "Electricity" ELECTRICITY
ITEM          "Gas" GAS
GOTO          CONTACTS

# WATER
SELECT        "water" "Water service"
```

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE         "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

```
....
GOTO Hello  // The program jumps to message hello world after executing this command.
...
...
# Hello
MESSAGE "Hello" "Hello world"
...
```

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

```
SELECT  <parameter name> <title>
ITEM    <item name>
ITEM    <item name>
ITEM    <item name>

SELECT_MULTI < parameter name> <title>
ITEM    <item name>
```

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

```
BRANCH_TO    <parameter name> <title>
ITEM         <item> <label>
ITEM         <item > <label>
ITEM         <item > <label>
```

Where:

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

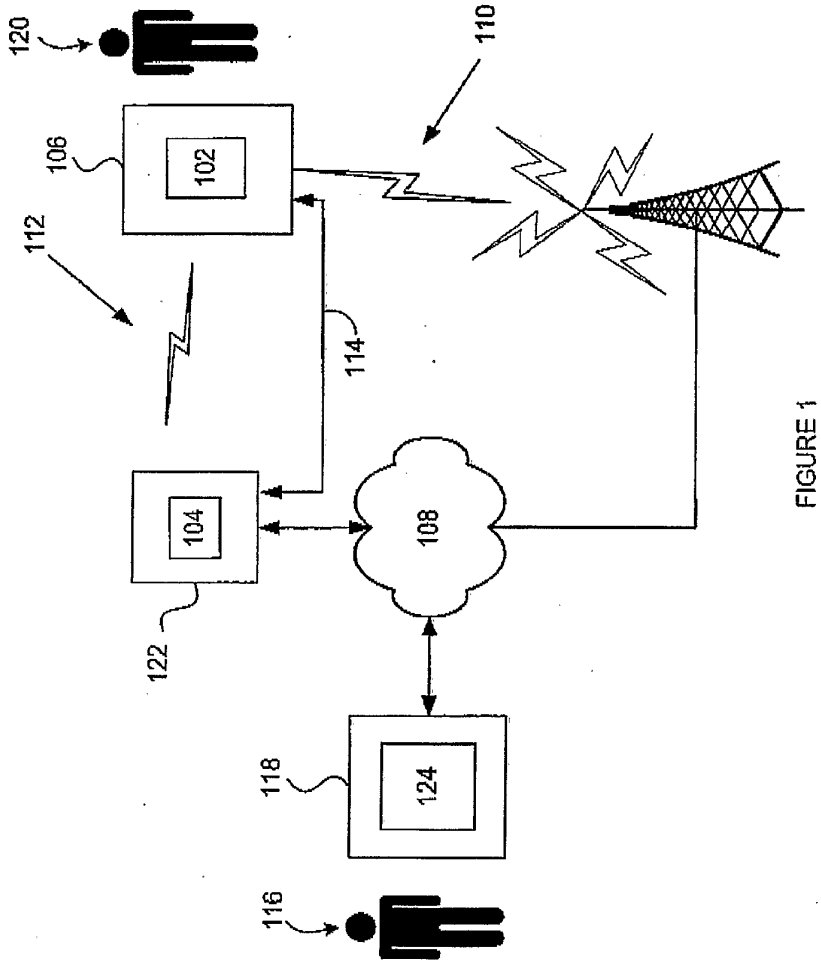


FIGURE 1

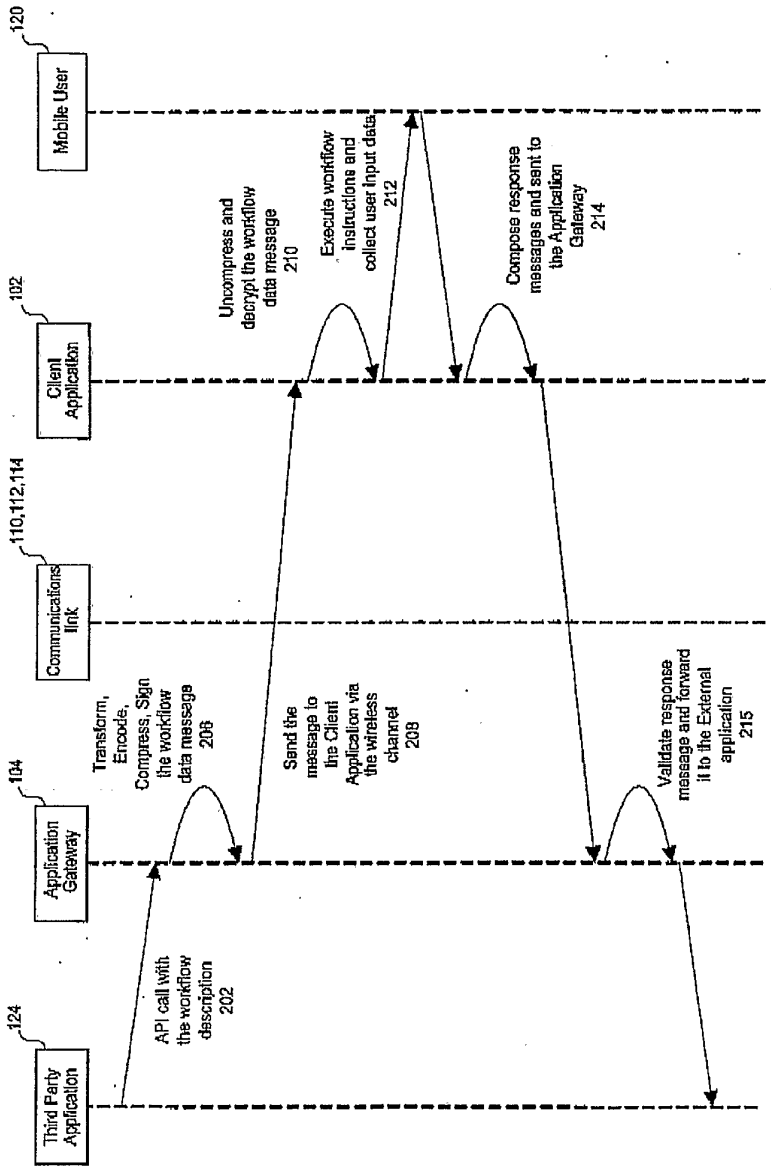

120
Mobile User
102
Client Application
110,112,114
Communications link
104
Application Gateway
124
Third Party Application
API call with the workflow description 202
Transform, Encode, Compress, Sign the workflow data message 206
Send the message to the Client Application via the wireless channel 208
Uncompress and decrypt the workflow data message 210
Execute workflow instructions and collect user input data 212
Compose response messages and sent to the Application Gateway 214
Validate response message and forward it to the External application 215

FIGURE 2

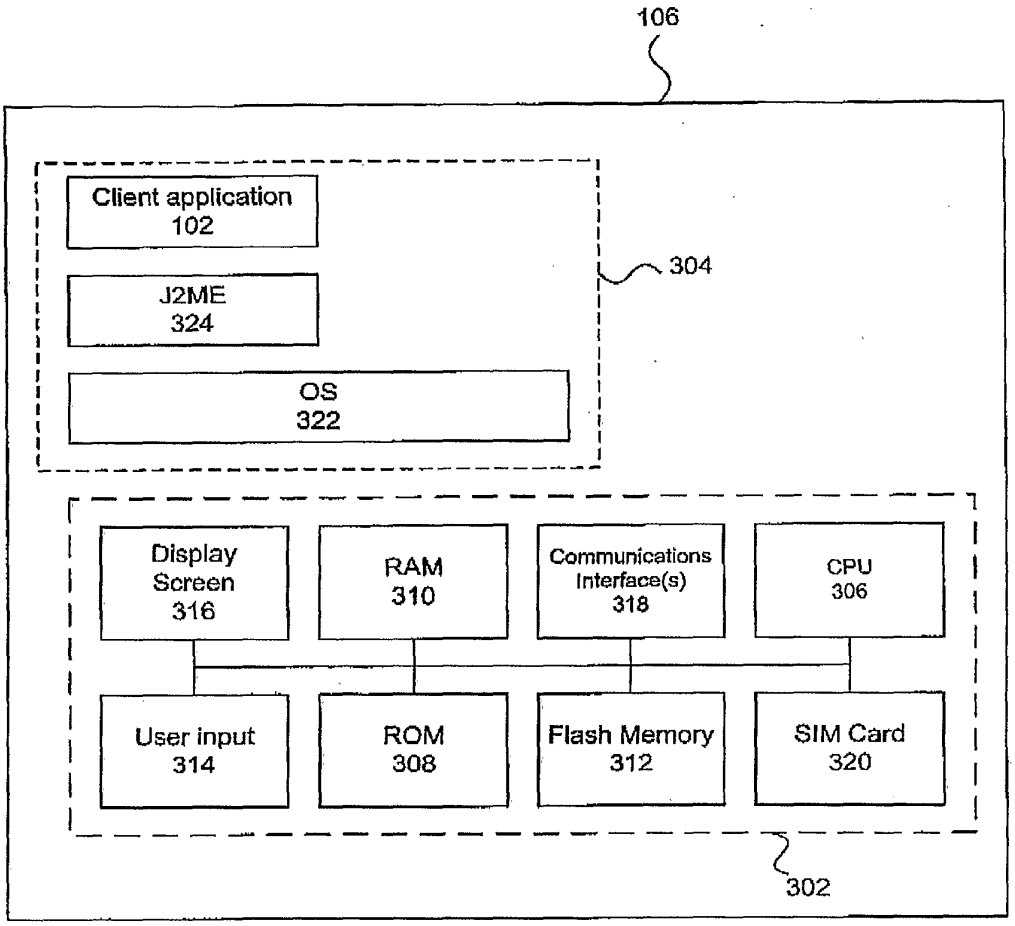

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

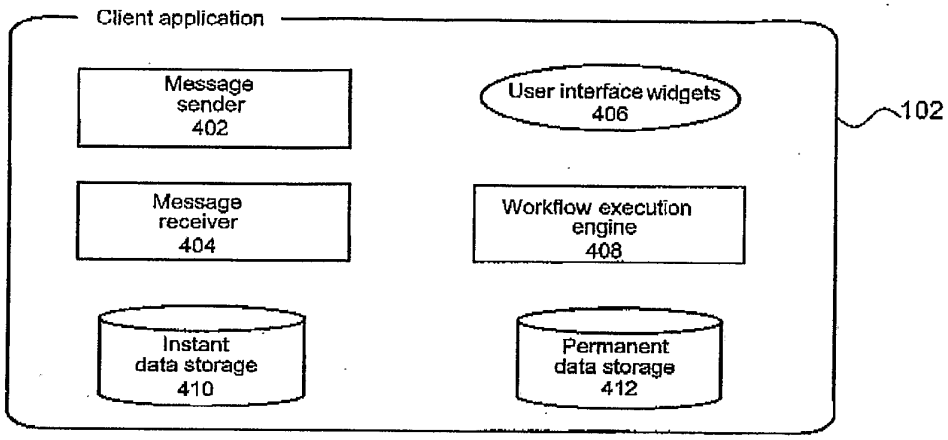


FIGURE 4



FIGURE 5

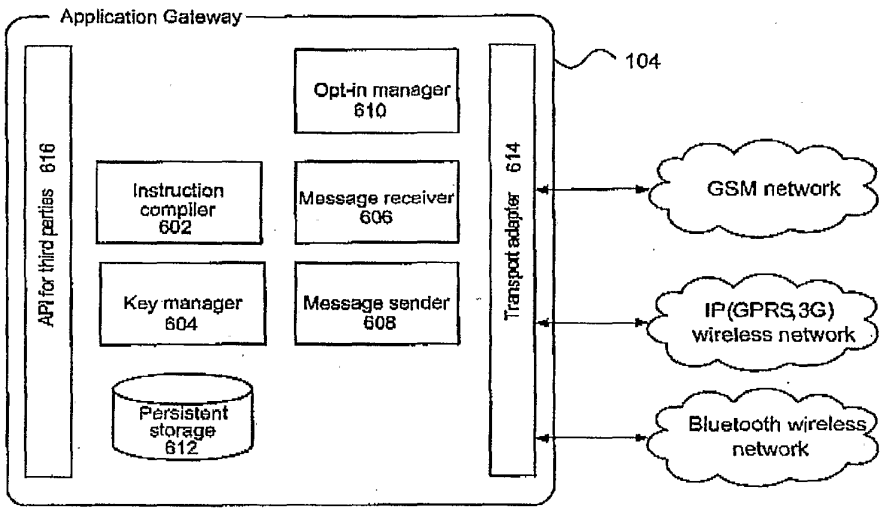

Application Gateway
API for third parties 616
Instruction compiler 602
Key manager 604
Persistent storage 612
Opt-in manager 610
Message receiver 606
Message sender 608
Transport adapter 614
104
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

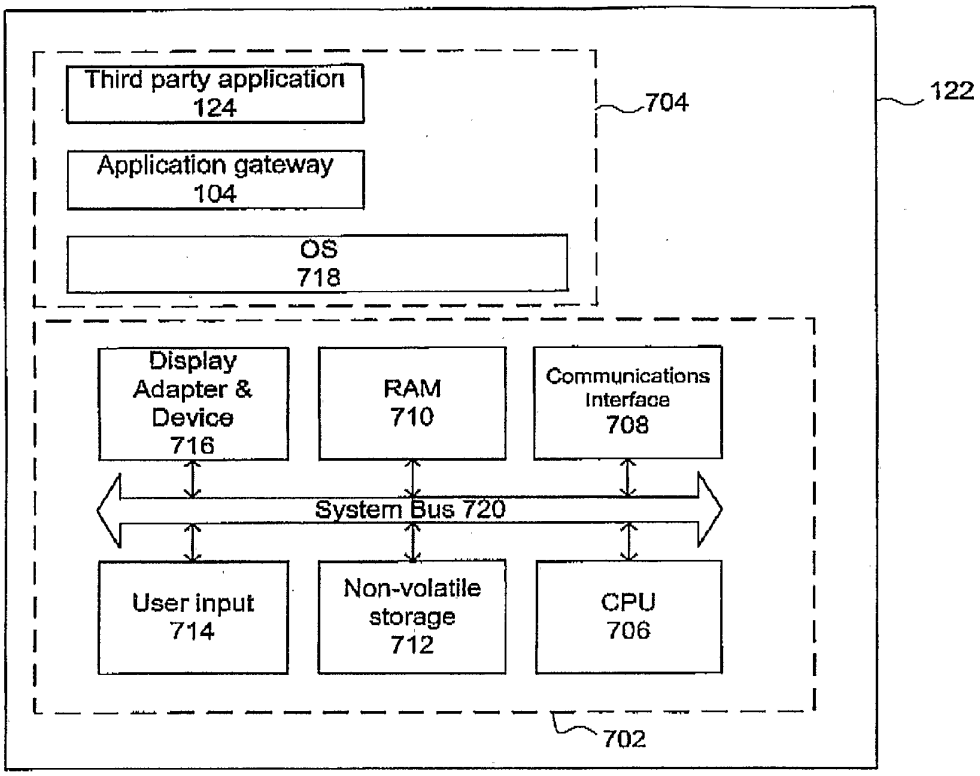

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

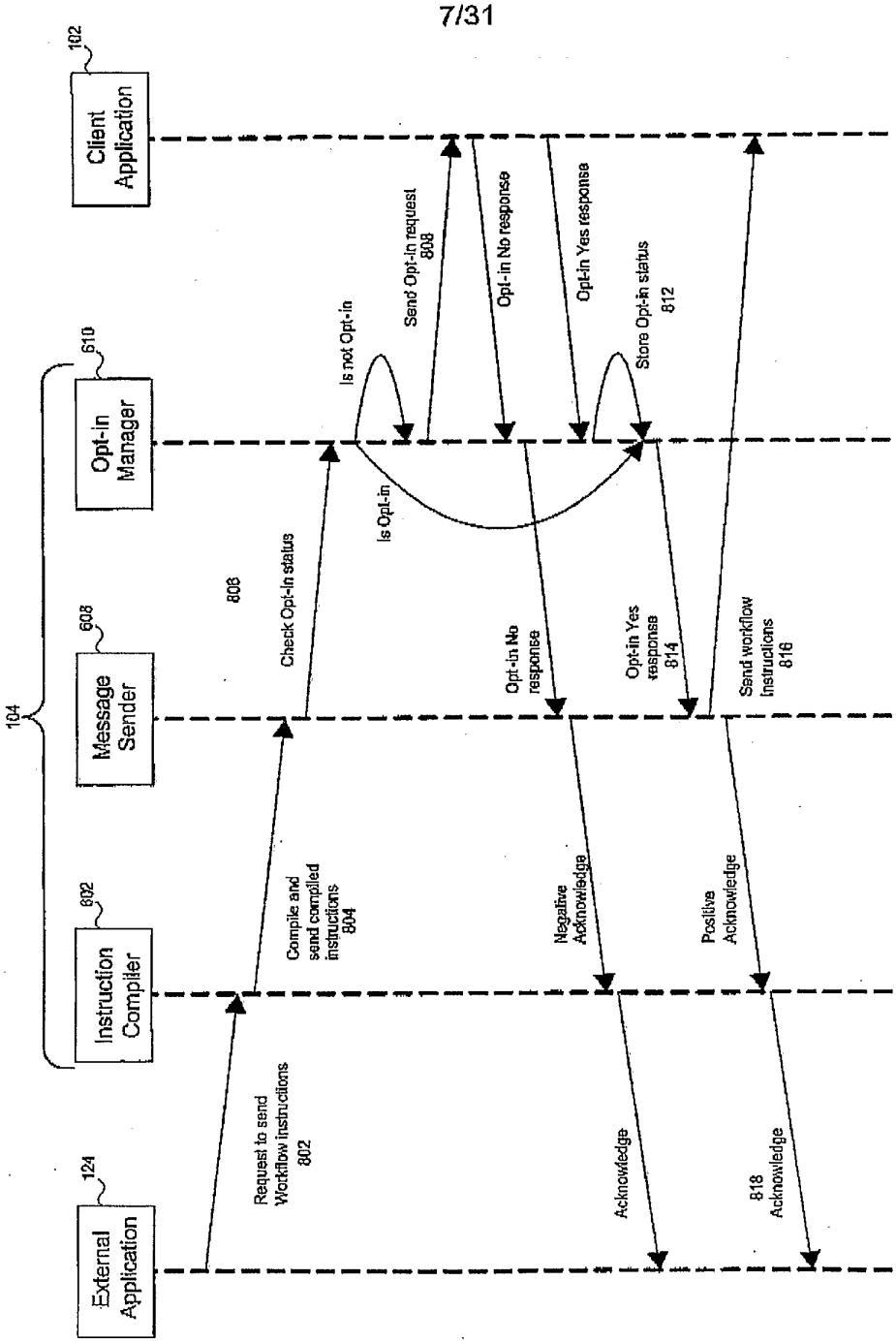

102
Client Application
610
Opt-in Manager
608
Message Sender
602
Instruction Compiler
124
External Application
104
Is not Opt-in
Send Opt-in request 808
Opt-in No response
Opt-in Yes response
Store Opt-in status 812
Is Opt-in
806
Check Opt-in status
Opt-in No response
Opt-in Yes response 814
Send workflow instructions 816
Compile and send compiled instructions 804
Negative Acknowledge
Positive Acknowledge
Request to send Workflow instructions 802
Acknowledge
818 Acknowledge

Figure 8

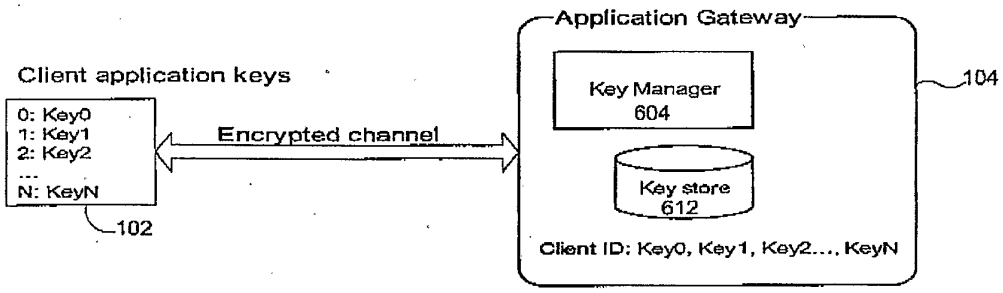

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

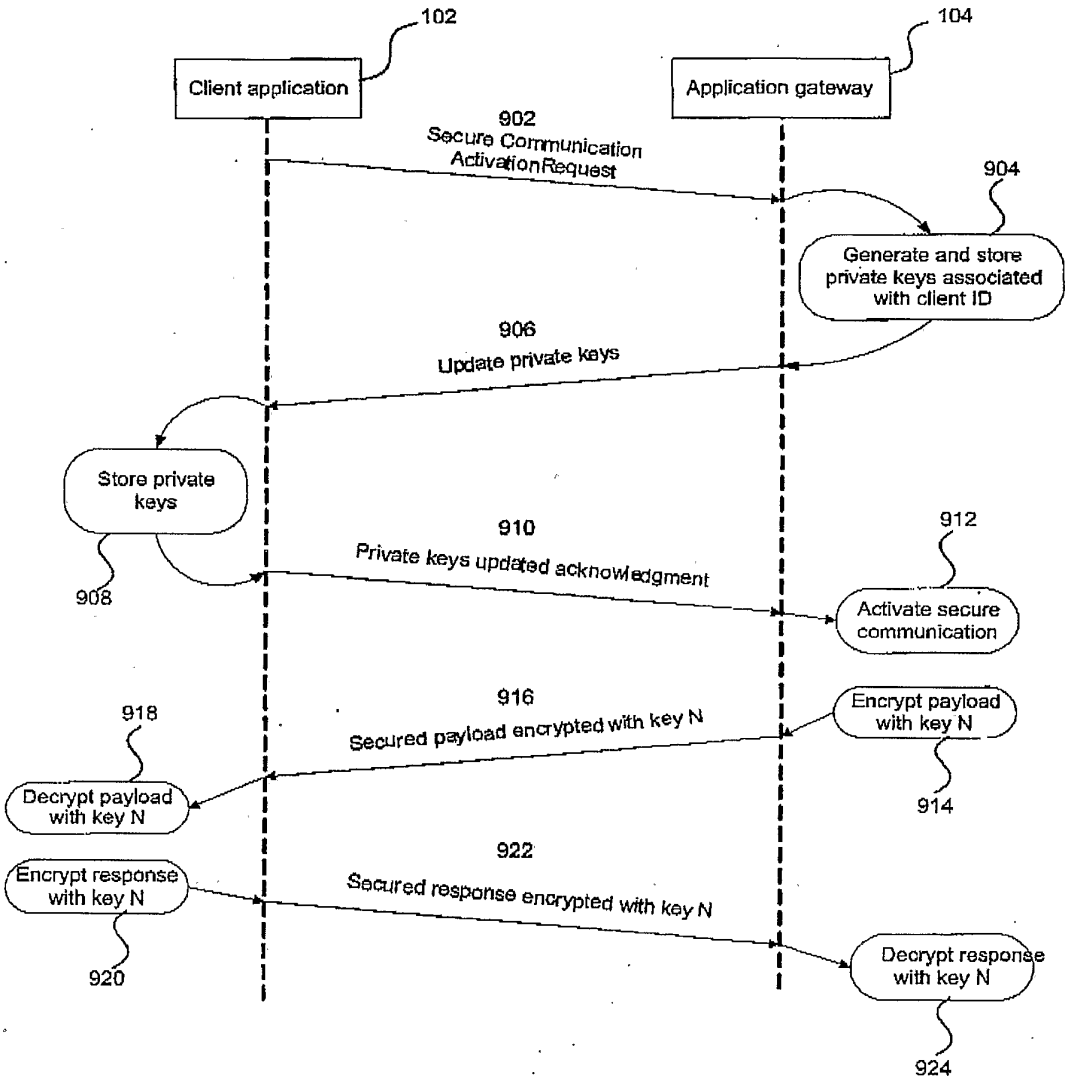

102
Client application
104
Application gateway
902
Secure Communication ActivationRequest
904
Generate and store private keys associated with client ID
906
Update private keys
Store private keys
908
910
Private keys updated acknowledgment
912
Activate secure communication
916
Secured payload encrypted with key N
Encrypt payload with key N
914
918
Decrypt payload with key N
922
Secured response encrypted with key N
Encrypt response with key N
920
Decrypt response with key N
924

FIGURE 10

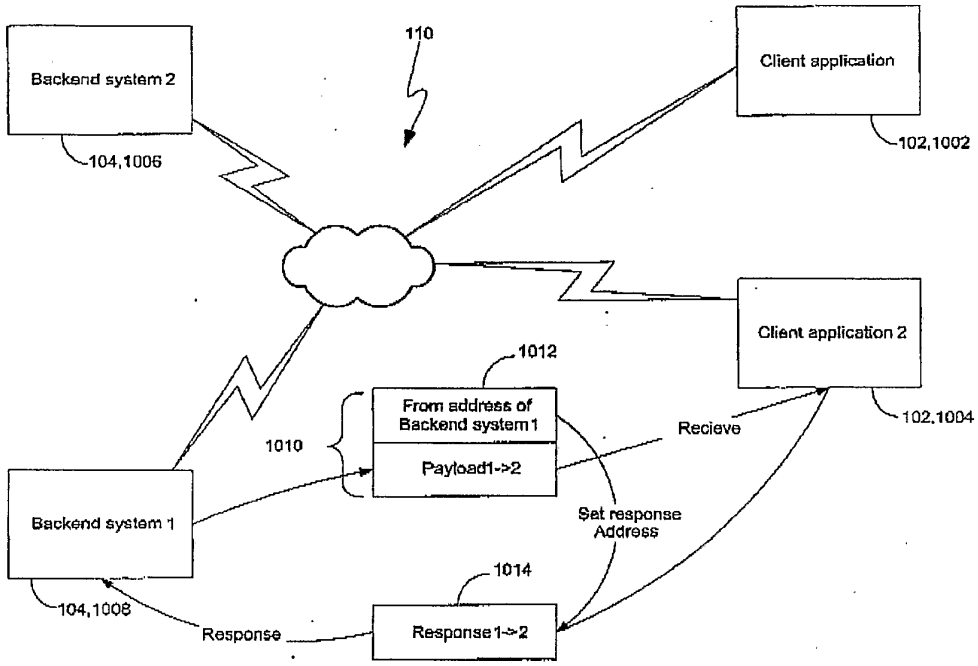

110
Backend system 2
104,1006
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Backend system 1
Set response Address
1014
104,1008
Response
Response 1->2

FIGURE 11

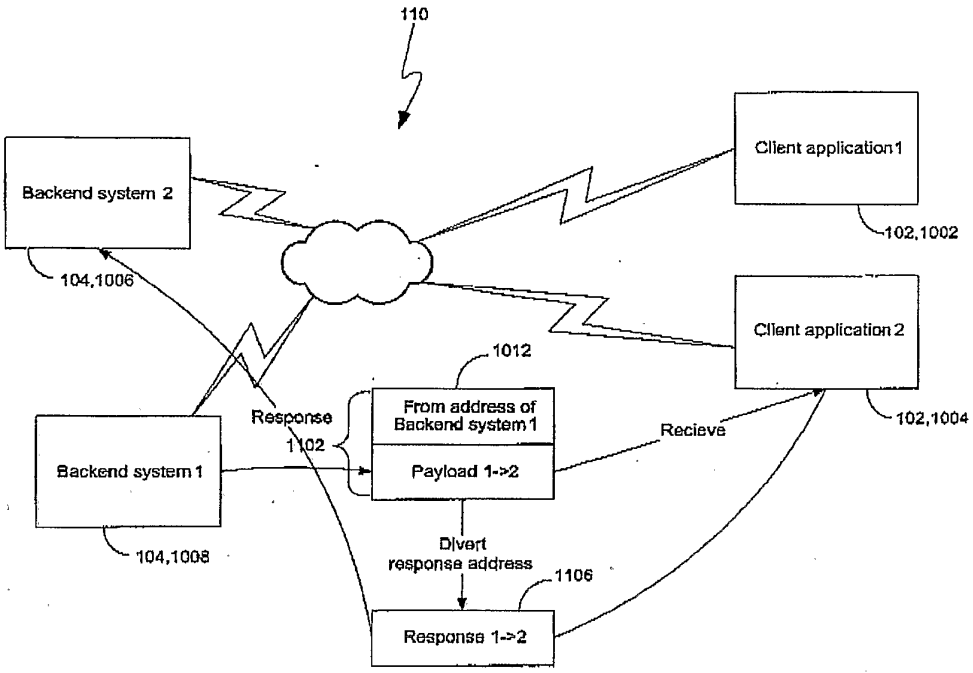

110
Backend system 2
Client application1
102,1002
104,1006
Client application 2
1012
From address of Backend system 1
Response 1102
Recieve
102,1004
Backend system 1
Payload 1->2
104,1008
Divert response address
1106
Response 1->2

FIGURE 12

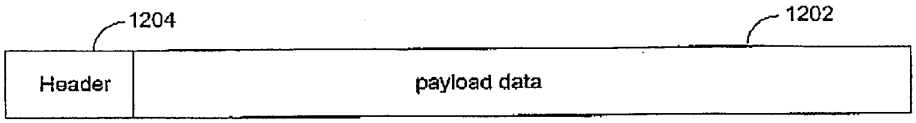


FIGURE 13

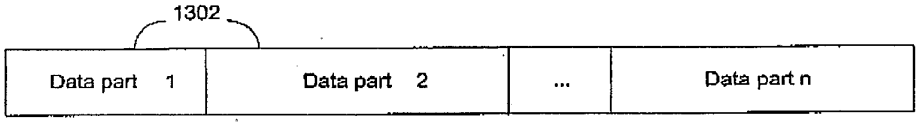


FIGURE 14

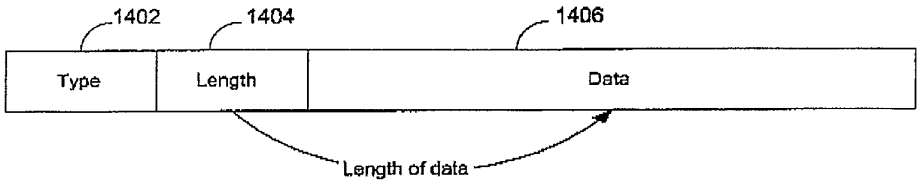


FIGURE 15

Workflow instruction data structure

	Type	Data
Menu Single/Multiple Select	S,M	[PARAMETER] [TITLE] [ITEM1] [ITEM2]..... [ITEMn]
Information Message	I	[TITLE] [MESSAGE]
Header Response	H	[HEADER]
Redirect Address	R	[PHONE NUMBER]
User Input	T	[PARAMETER] [LABEL] [TYPE]
Execute URL	E	[URL]
Jump to index	J	[CMD index]
Go to previous Cmd	P	
Branch menu	B	[PARAMETER] [TITLE] [Label1,index1] [Label2, index2] ..... [ITEMn]
No-op	N	
Store Permanent	K	[Title]
Clear Permanent Storage	D	
Read System Property	P	[Property name]
Configuration Settings	C	[Configurations]

Type enumeration:
TYPE_ANY = 0;
TYPE_EMAILADDR=1;
TYPE_NUMERIC = 2;
TYPE_PHONENUMBER = 3;
TYPE_URL = 4;
TYPE_DECIMAL = 5;

FIGURE 16

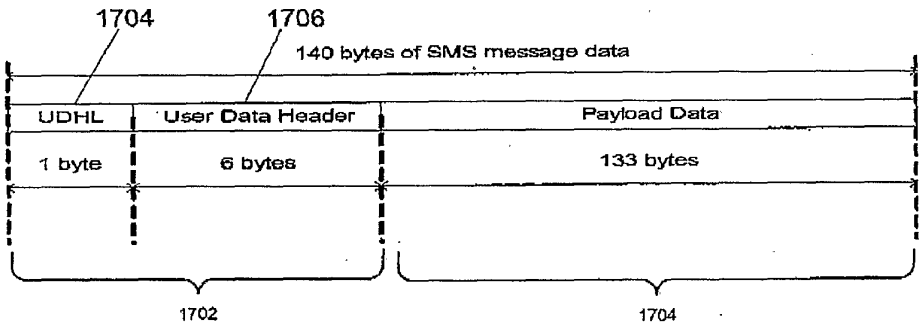

1704
1706
140 bytes of SMS message data
UDHL
User Data Header
Payload Data
1 byte
6 bytes
133 bytes
1702
1704

FIGURE 17

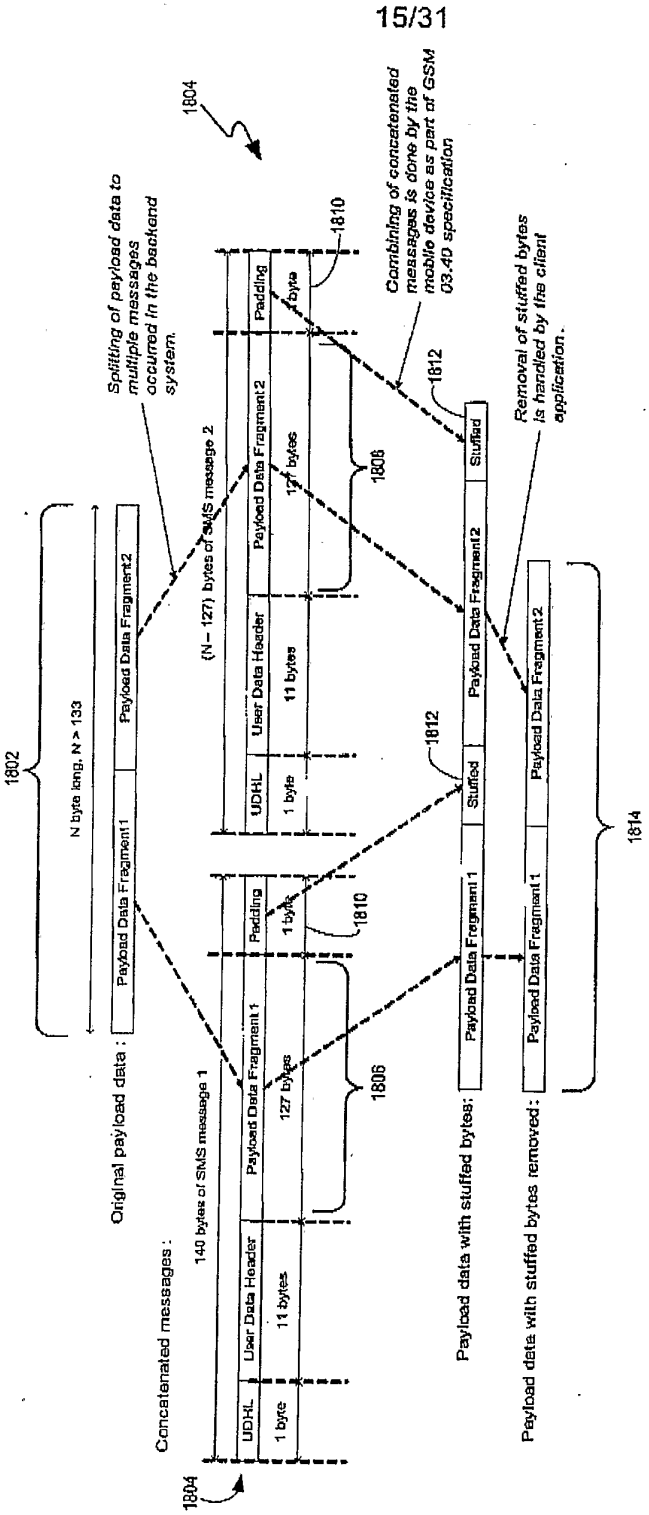

1802
N byte long, N > 133
Payload Data Fragment1
Payload Data Fragment2
Original payload data :
Splitting of payload data to multiple messages occurred in the backend system.
1804
(N – 127) bytes of SMS message 2
UDHL
User Data Header
Payload Data Fragment2
Padding
1 byte
11 bytes
127 bytes
1 byte
1810
1806
1812
Combining of concatenated messages is done by the mobile device as part of GSM 03.40 specification
Stuffed
Payload data with stuffed bytes:
Removal of stuffed bytes is handled by the client application.
Payload data with stuffed bytes removed:
1814
Concatenated messages :
140 bytes of SMS message 1
Payload Data Fragment 1

FIGURE 18

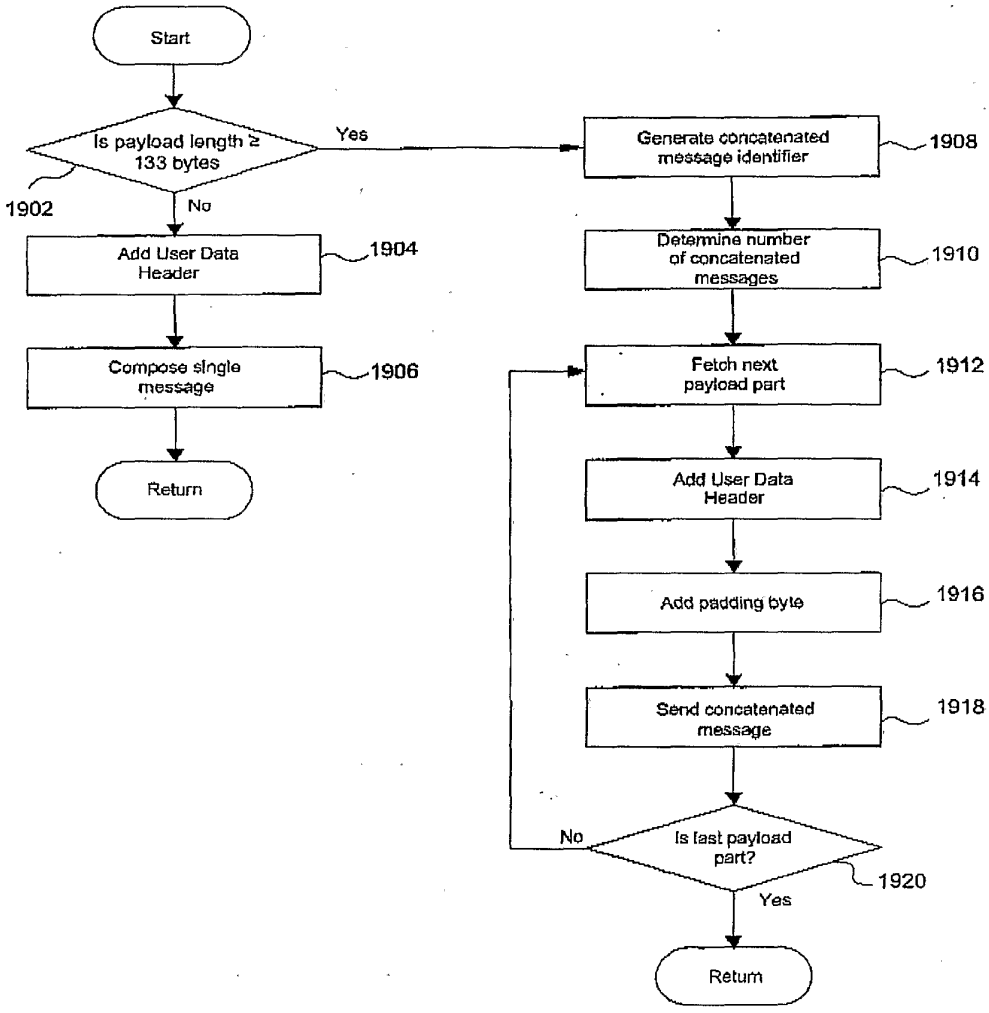

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
No
Yes
1920
Return

FIGURE 19

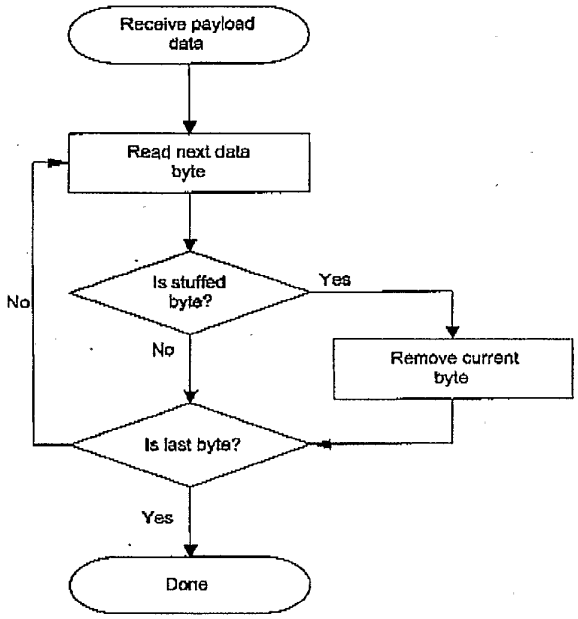

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
No
Is last byte?
Yes
Done

FIGURE 20

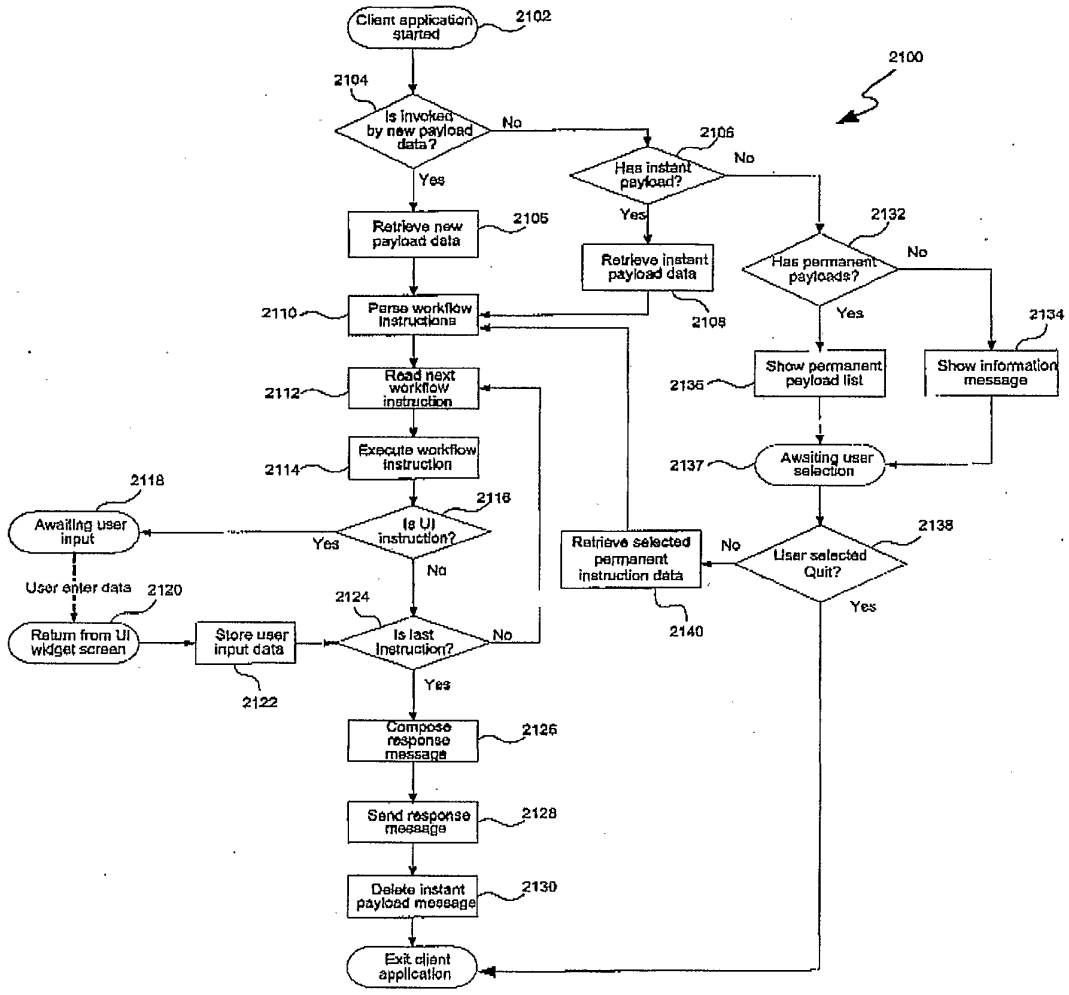

Client application started
2102
2100
2104
Is invoked by new payload data?
No
2106
Has instant payload?
No
Yes
Yes
Retrieve new payload data
2105
Retrieve instant payload data
2108
2132
Has permanent payloads?
No
Yes
2134
2110
Parse workflow instructions
Show permanent payload list
2136
Show information message
2112
Read next workflow instruction
2114
Execute workflow instruction
2137
Awaiting user selection
2118
2116
Awaiting user input
Is UI instruction?
Yes
No
2138
Retrieve selected permanent instruction data
No
User selected Quit?
Yes
2140
User enter data
2120
2124
Return from UI widget screen
Store user input data
Is last Instruction?
No
Yes
2122
Compose response message
2126
Send response message
2128
Delete instant payload message
2130
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

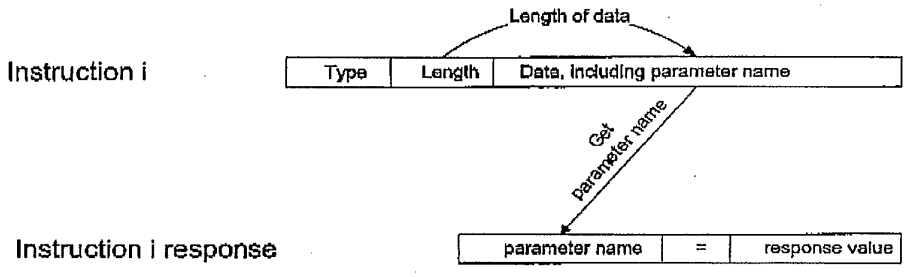


FIGURE 23

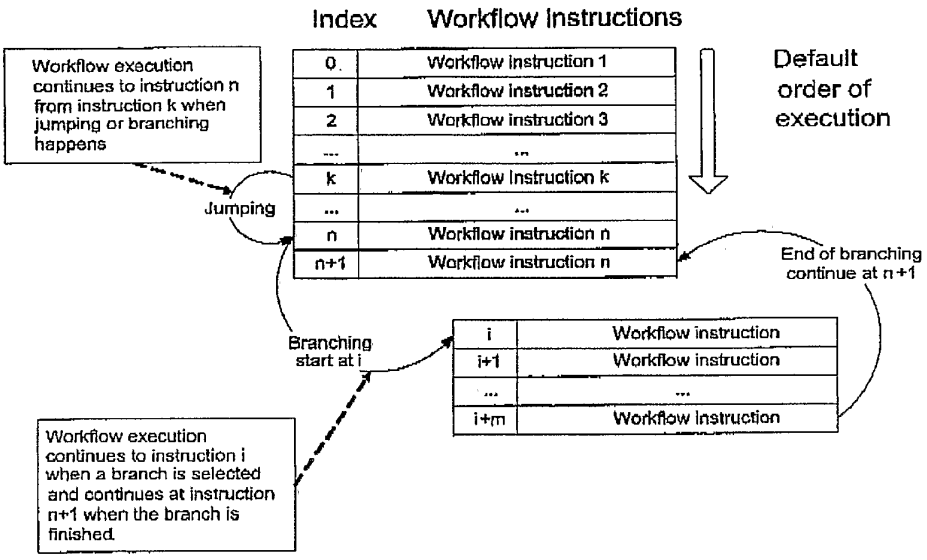

Index
Workflow Instructions
Workflow execution continues to instruction n from instruction k when jumping or branching happens
0
Workflow instruction 1
1
Workflow instruction 2
2
Workflow instruction 3
k
Workflow instruction k
n
Workflow instruction n
n+1
Workflow instruction n
Default order of execution
Jumping
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished.

FIGURE 24

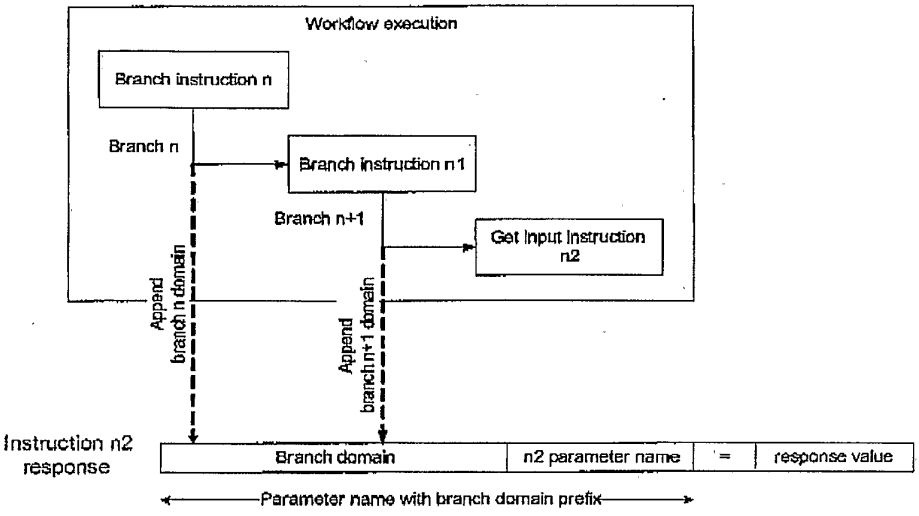

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get Input Instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

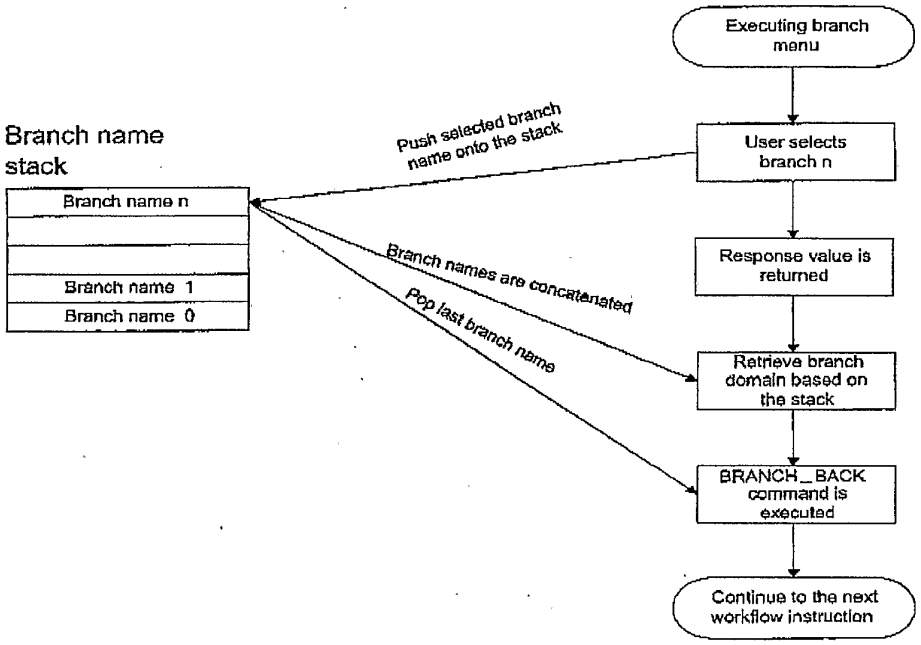

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name
Branch name stack
Branch name n
Branch name 1
Branch name 0

FIGURE 26

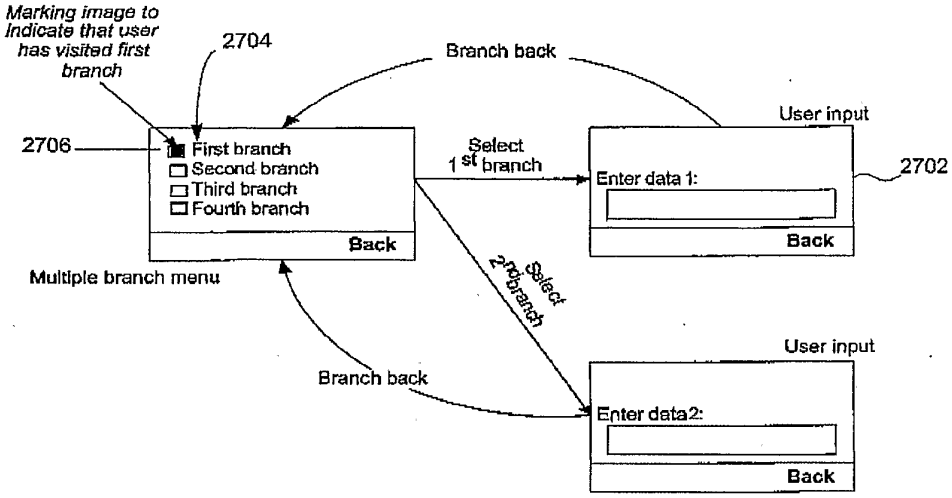


FIGURE 27

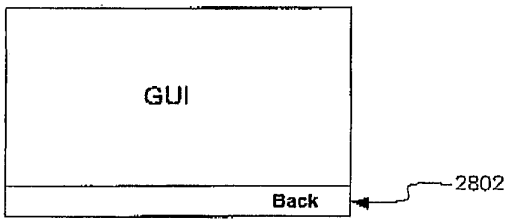


FIGURE 28

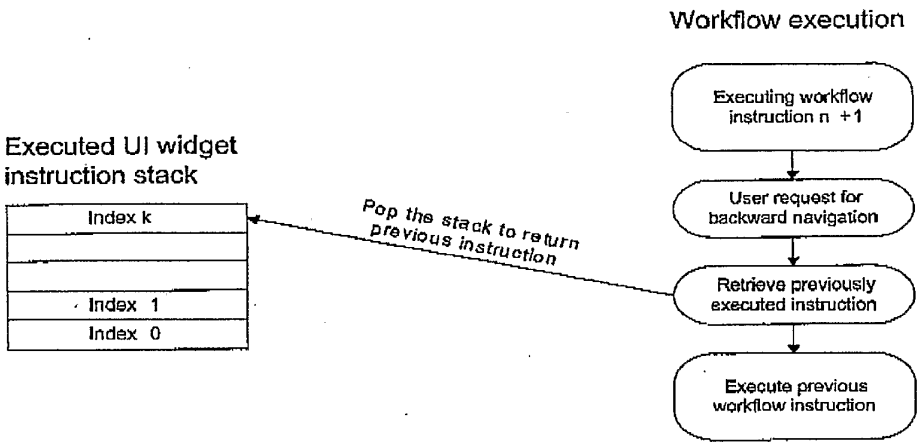

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

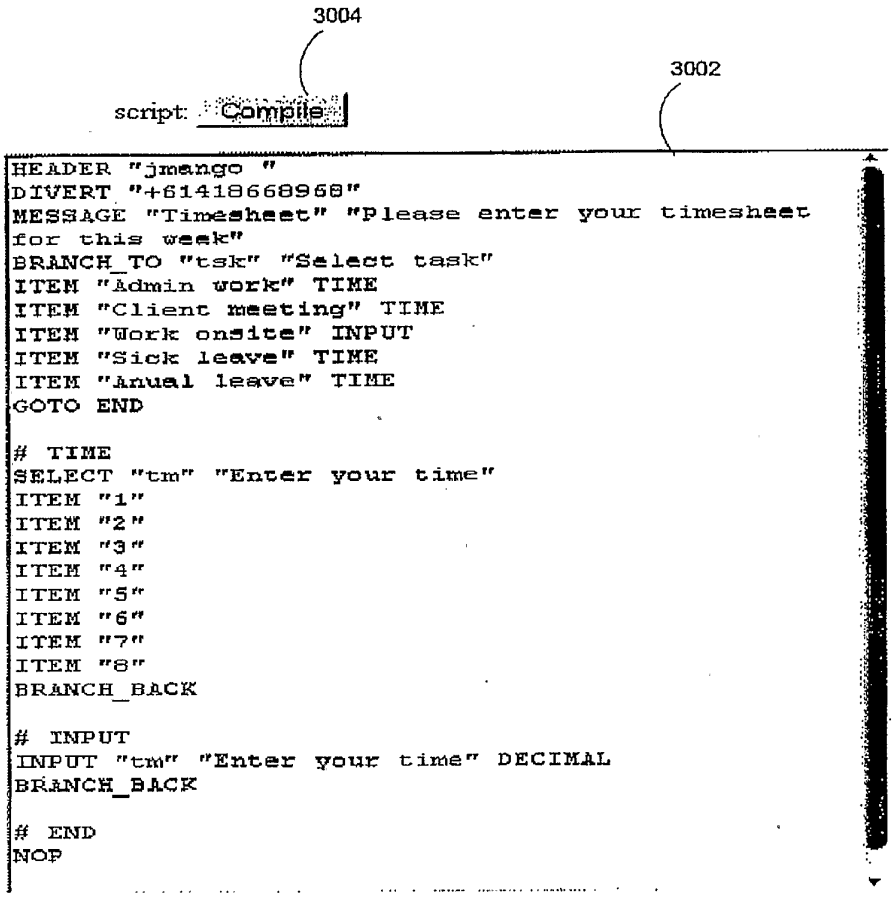

3004
3002
script:
Compile
HEADER "jmango "
DIVERT "+61418668968"
MESSAGE "Timesheet" "Please enter your timesheet
for this week"
BRANCH_TO "tsk" "Select task"
ITEM "Admin work" TIME
ITEM "Client meeting" TIME
ITEM "Work onsite" INPUT
ITEM "Sick leave" TIME
ITEM "Anual leave" TIME
GOTO END
TIME
SELECT "tm" "Enter your time"
ITEM "1"
ITEM "2"
ITEM "3"
ITEM "4"
ITEM "5"
ITEM "6"
ITEM "7"
ITEM "8"
BRANCH_BACK
INPUT
INPUT "tm" "Enter your time" DECIMAL
BRANCH_BACK
END
NOP

FIGURE 30

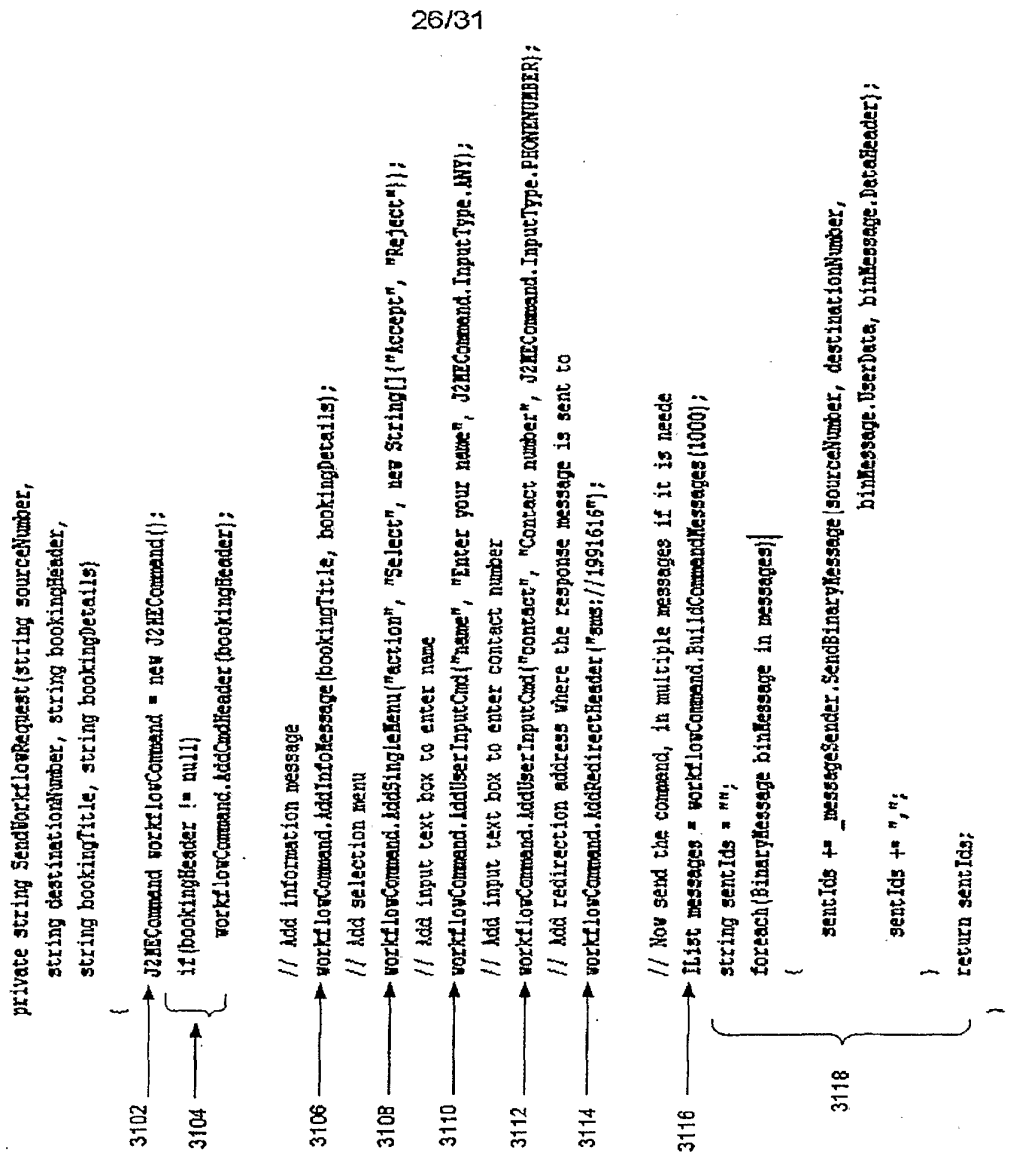

private string SendWorkflowRequest(string sourceNumber,
string destinationNumber, string bookingHeader,
string bookingTitle, string bookingDetails)
{
3102 J2MECommand workflowCommand = new J2MECommand();
3104 if(bookingHeader != null)
workflowCommand.AddCmdHeader(bookingHeader);
// Add information message
3106 workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
// Add selection menu
3108 workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
// Add input text box to enter name
3110 workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
// Add input text box to enter contact number
3112 workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
// Add redirection address where the response message is sent to
3114 workflowCommand.AddRedirectHeader("sms://1991616");
// Now send the command, in multiple messages if it is neede
3116 IList messages = workflowCommand.BuildCommandMessages(1000);
string sentIds = "";
foreach(BinaryMessage binMessage in messages)
{
3118 sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
binMessage.UserData, binMessage.DataHeader);
sentIds += ",";
}
return sentIds;
}

FIGURE 31

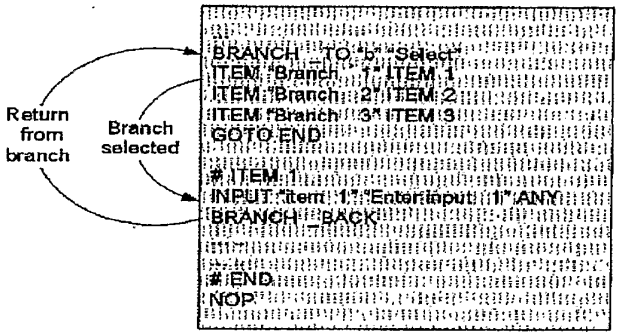


FIGURE 32

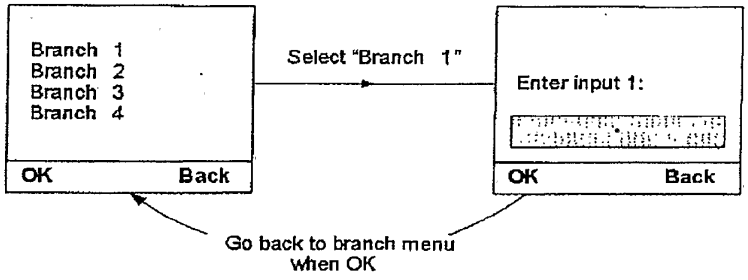


FIGURE 33

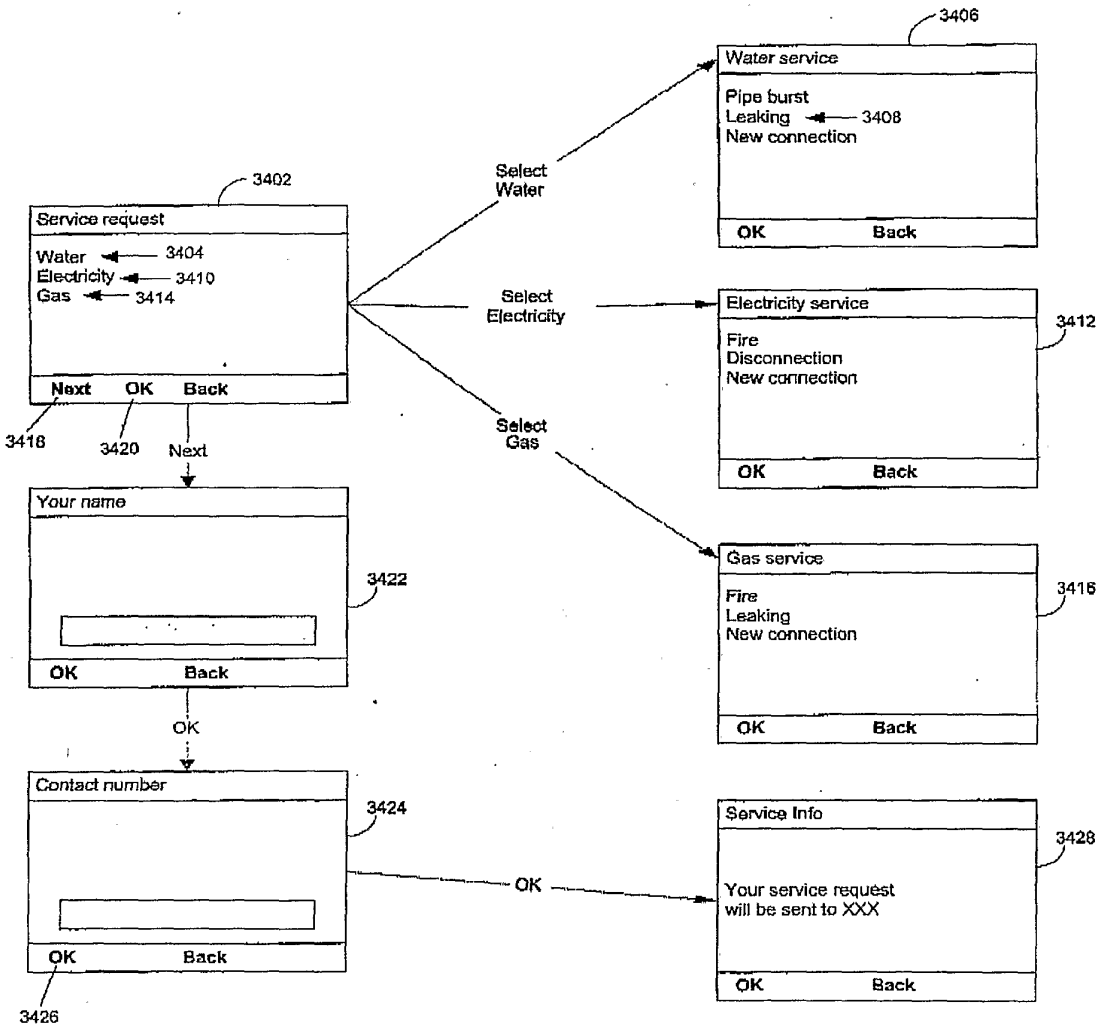

3406
Water service
Pipe burst
Leaking
3408
New connection
OK
Back
3402
Service request
Water
3404
Electricity
3410
Gas
3414
Next
OK
Back
3418
3420
Next
Select Water
Select Electricity
Select Gas
Electricity service
Fire
Disconnection
New connection
OK
Back
3412
Your name
3422
OK
Back
OK
Gas service
Fire
Leaking
New connection
OK
Back
3416
Contact number
3424
OK
Back
3426
OK
Service Info
Your service request will be sent to XXX
OK
Back
3428

FIGURE 34

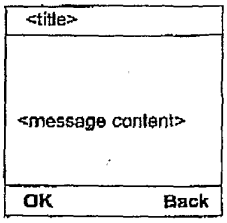


FIGURE 35

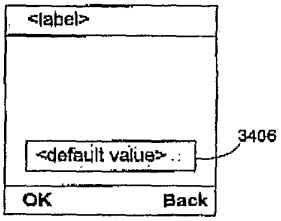


FIGURE 36

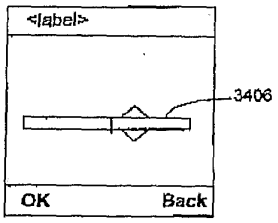


FIGURE 37

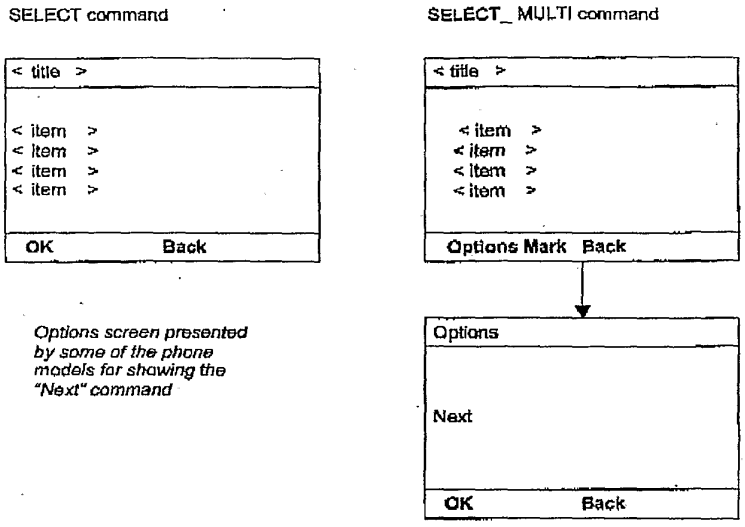

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

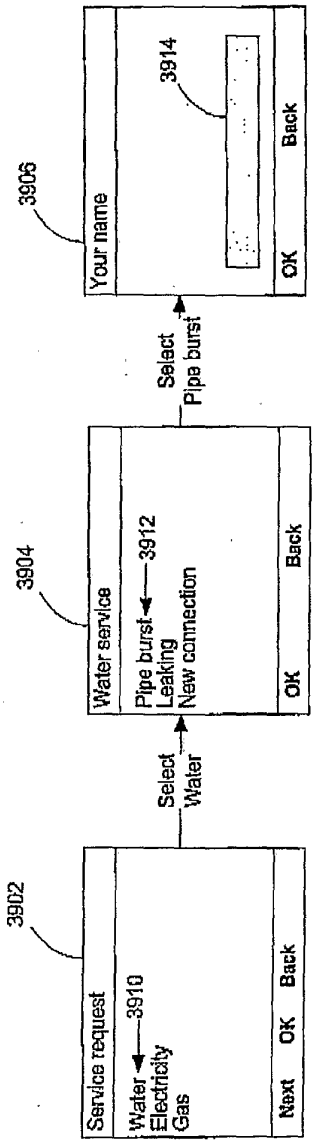

3902
Service request
Water
Electricity
Gas
3910
Next
OK
Back
Select
Water
3904
Water service
Pipe burst
Leaking
New connection
3912
OK
Back
Select
Pipe burst
3906
Your name
3914
OK
Back

FIGURE 39

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001599

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04Q 7/22 (2006.01) ***H04M 3/493*** (2006.01)

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 & USPTO: Keywords: (interactive, SMS, encryption, compile, header, payload and like 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 2006/0095291 A1 (Cherney) 4 May 2006. See for example the title; abstract; fig 4A-4C, 5 and 7; paras [0013]-[0016], [0033]-[0041], [0057]-[0080] and [0089]-[0140].	1-25
X	EP 1509049 A1 (Accenture Global Services GMBH) 20 August 2003. See for example the abstract; paras [0033]-[0039]; and fig 2 and 5.	1-25
A	US 2002/0073023 A1 (Castro et al.) 13 June 2002.	

☐ 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 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
11 December 2007	20 DEC 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Malcolm Peh** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 7914

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2007/001599**

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	2006095291	EP	1836676	US	2006095290	WO	2006050413
EP	1509049	US	2007191032	WO	2005020609		
US	2002073023						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2666616 A1 2008/04/24

(21) 2 666 616

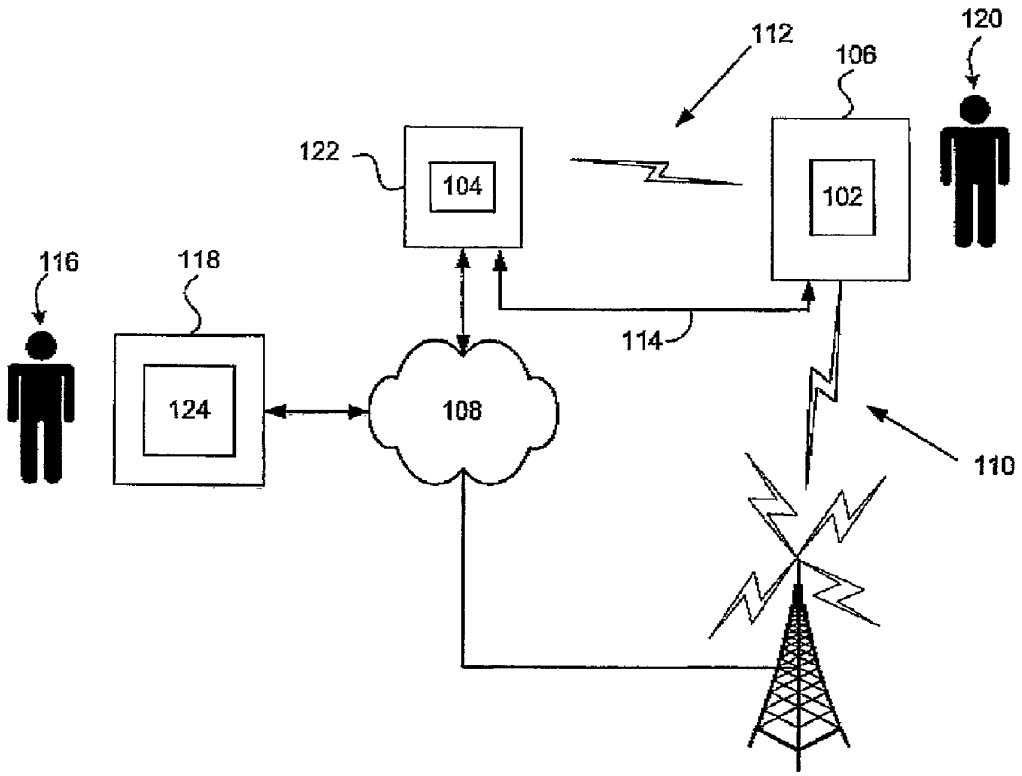
(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/10/19
(87) Date publication PCT/PCT Publication Date: 2008/04/24
(85) Entrée phase nationale/National Entry: 2009/04/15
(86) N° demande PCT/PCT Application No.: AU 2007/001599
(87) N° publication PCT/PCT Publication No.: 2008/046161
(30) Priorité/Priority: 2006/10/19 (AU2006905829)

(51) Cl.Int./Int.Cl. *H04W 4/12* (2009.01), *H04W 12/02* (2009.01), *H04W 12/06* (2009.01)
(71) Demandeur/Applicant:
FRUITFUL TECHNOLOGIES PTY LTD, AU
(72) Inventeur/Inventor:
NGO, DUC ANH, AU
(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : SYSTEME ET PROCEDE INTERACTIFS
(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abrégé/Abstract:
A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [—/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

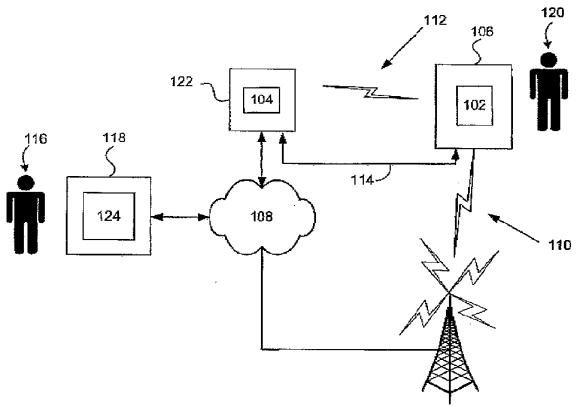
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(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, ME, 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).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;

(ii) interprets these instructions;

(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and

(iv) sends responses back to the gateway 104 or other computer system or device.

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
# START
BRANCH_TO     "serv" "Service Request"
ITEM          "Water" WATER
ITEM          "Electricity" ELECTRICITY
ITEM          "Gas" GAS
GOTO          CONTACTS

# WATER
SELECT        "water" "Water service"
```

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE     "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

....
GOTO Hello // The program jumps to message hello world after executing this command.
...
...
Hello
MESSAGE "Hello" "Hello world"
...

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

SELECT <parameter name> <title>
ITEM <item name>
ITEM <item name>
ITEM <item name>

SELECT_MULTI < parameter name> <title>
ITEM <item name>

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

```
BRANCH_TO    <parameter name> <title>
ITEM         <item> <label>
ITEM         <item > <label>
ITEM         <item > <label>
```

Where:

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

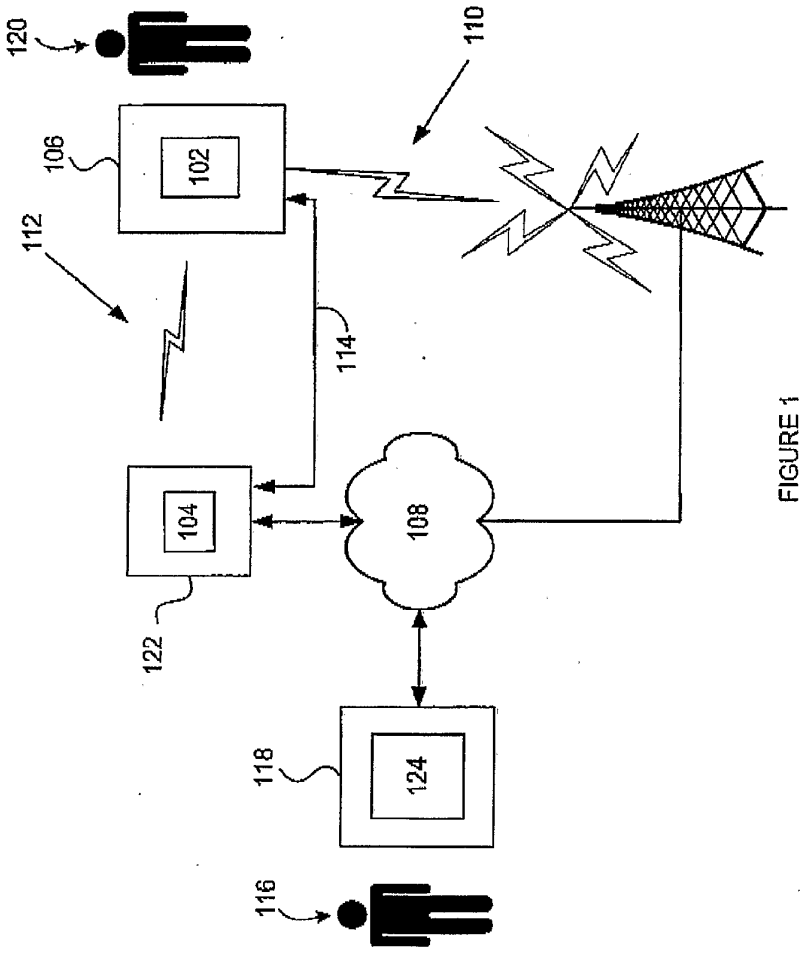


FIGURE 1

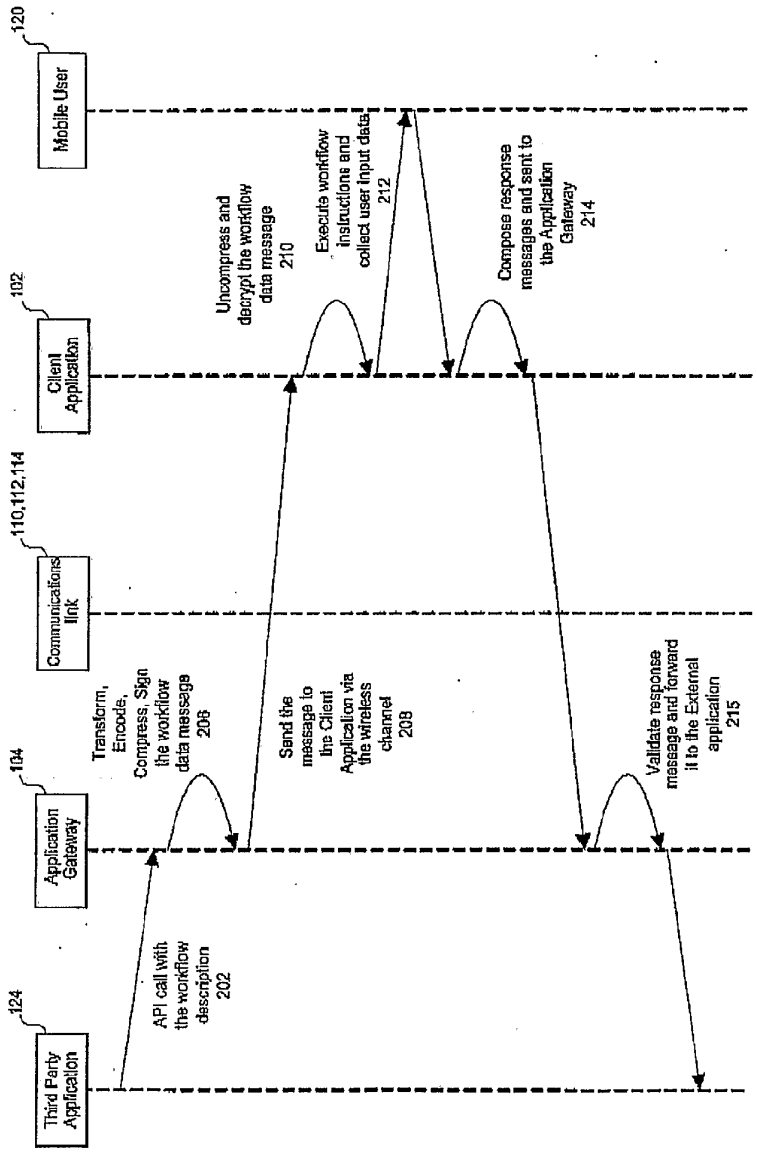

120
Mobile User
102
Client Application
110,112,114
Communications link
104
Application Gateway
124
Third Party Application
API call with the workflow description 202
Transform, Encode, Compress, Sign the workflow data message 206
Send the message to the Client Application via the wireless channel 208
Uncompress and decrypt the workflow data message 210
Execute workflow instructions and collect user input data 212
Compose response messages and sent to the Application Gateway 214
Validate response message and forward it to the External application 215

FIGURE 2

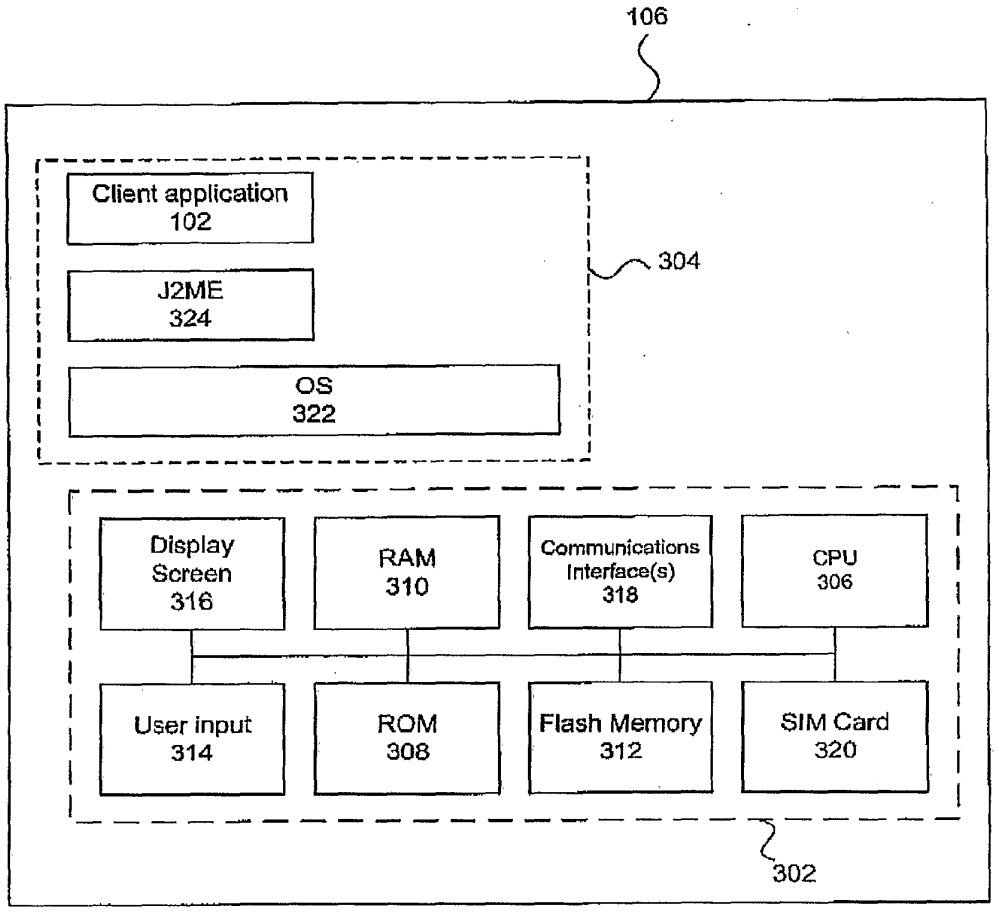

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

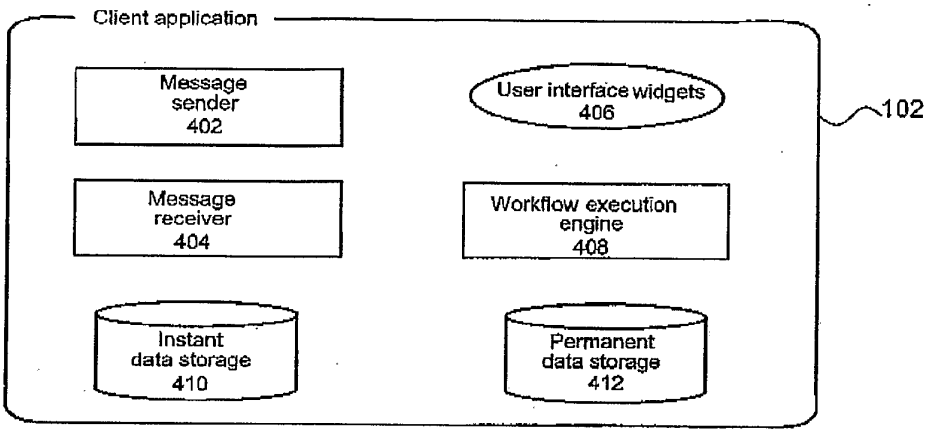


FIGURE 4



FIGURE 5

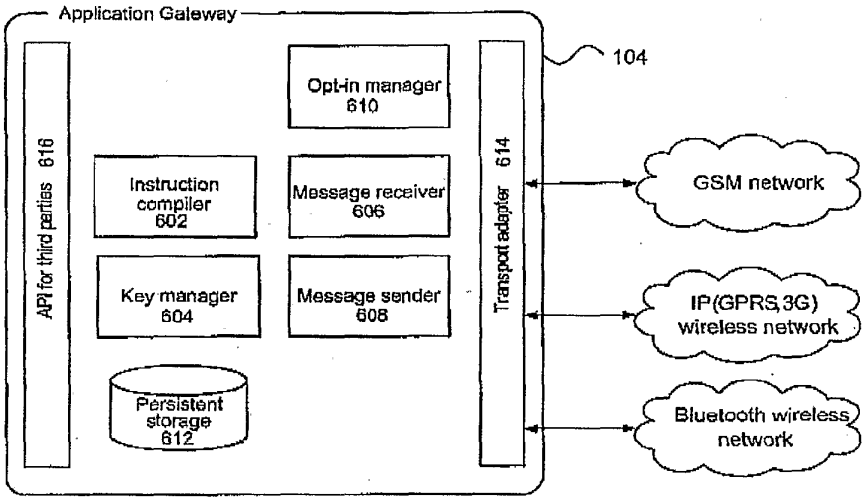

Application Gateway
104
API for third parties 616
Opt-in manager 610
Instruction compiler 602
Message receiver 606
Key manager 604
Message sender 608
Persistent storage 612
Transport adapter 614
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

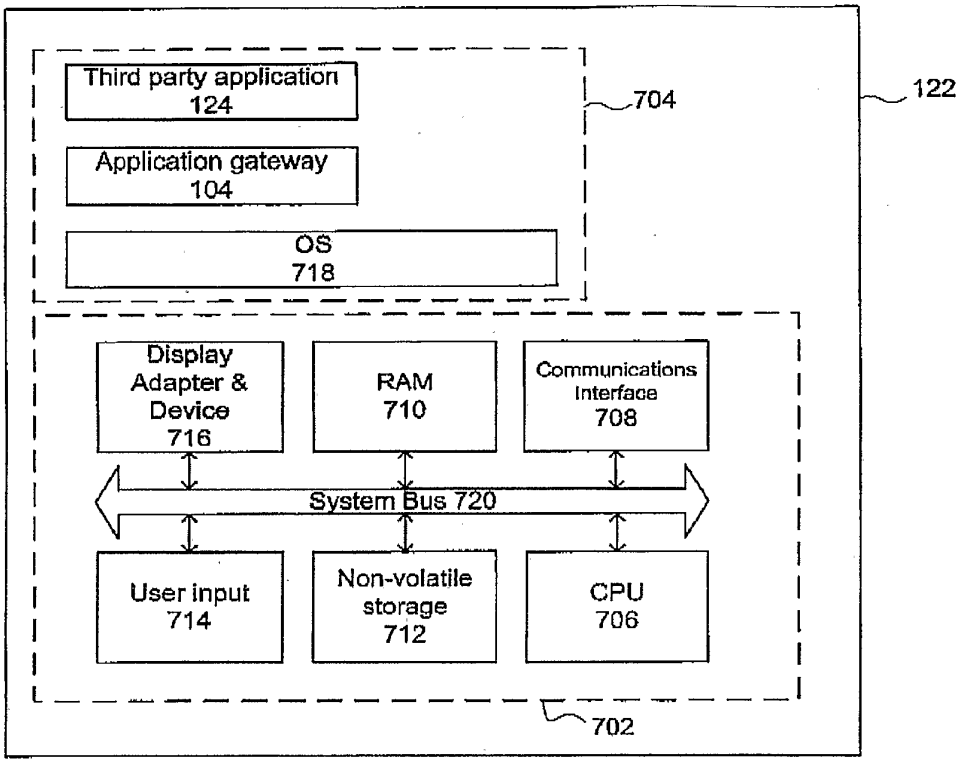

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

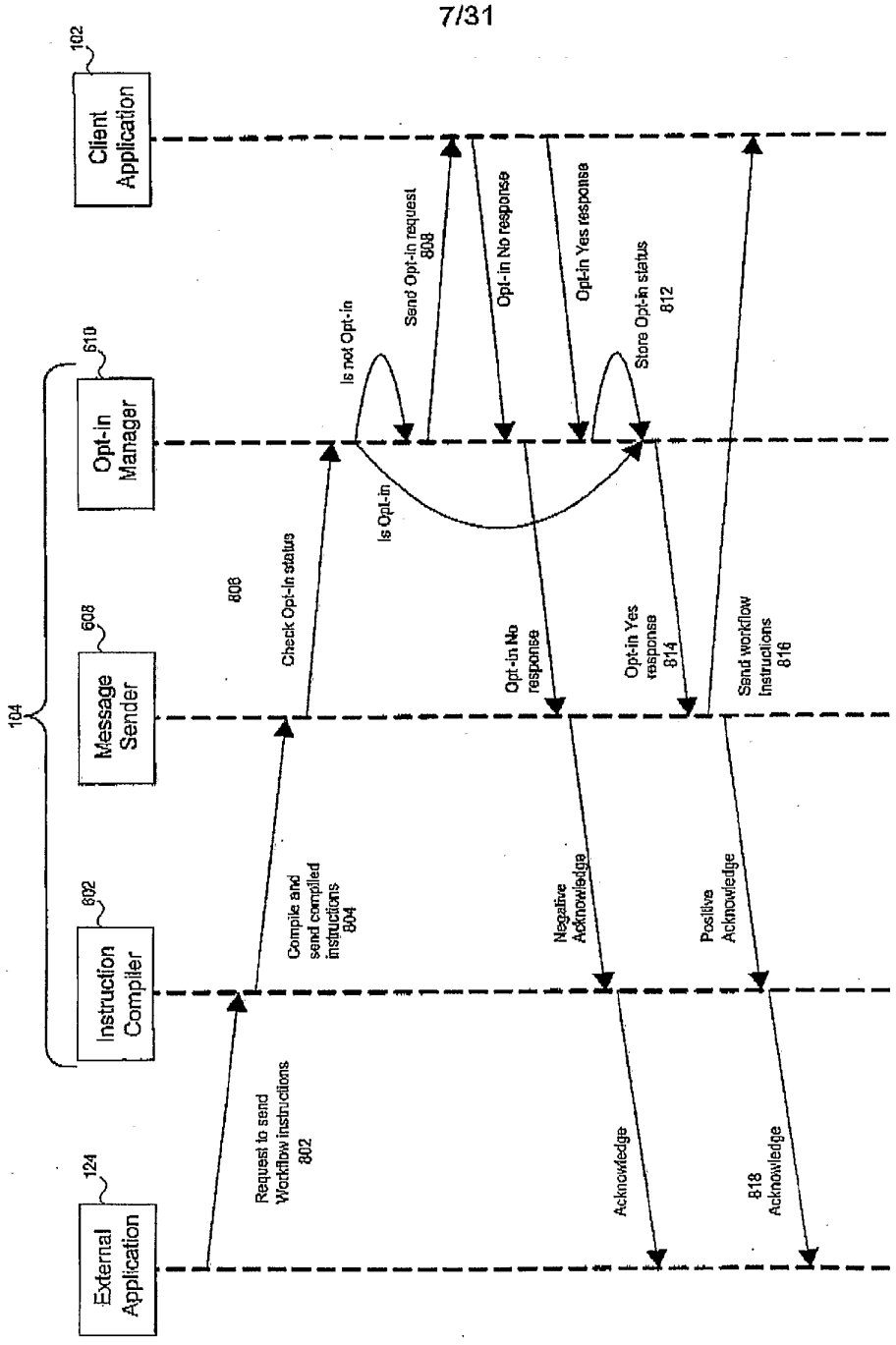

102
Client Application
610
Opt-in Manager
608
Message Sender
602
Instruction Compiler
124
External Application
104
Is not Opt-in
Send Opt-in request 808
Opt-in No response
Opt-in Yes response
Store Opt-in status 812
Is Opt-in
606
Check Opt-in status
Opt-in No response
Opt-in Yes response 814
Send workflow instructions 816
Compile and send compiled instructions 804
Negative Acknowledge
Positive Acknowledge
Request to send Workflow instructions 802
Acknowledge
818 Acknowledge

Figure 8

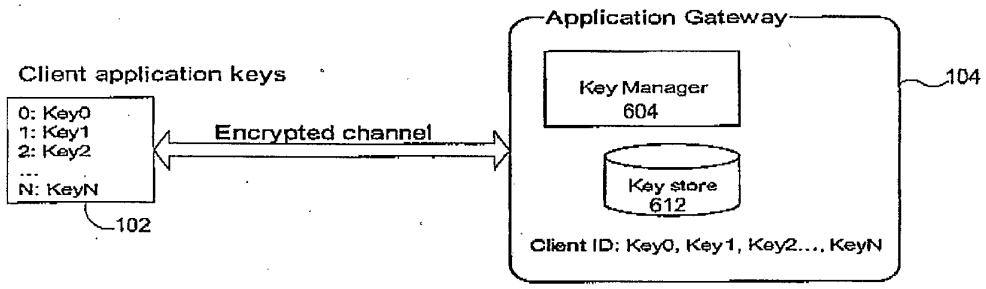

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

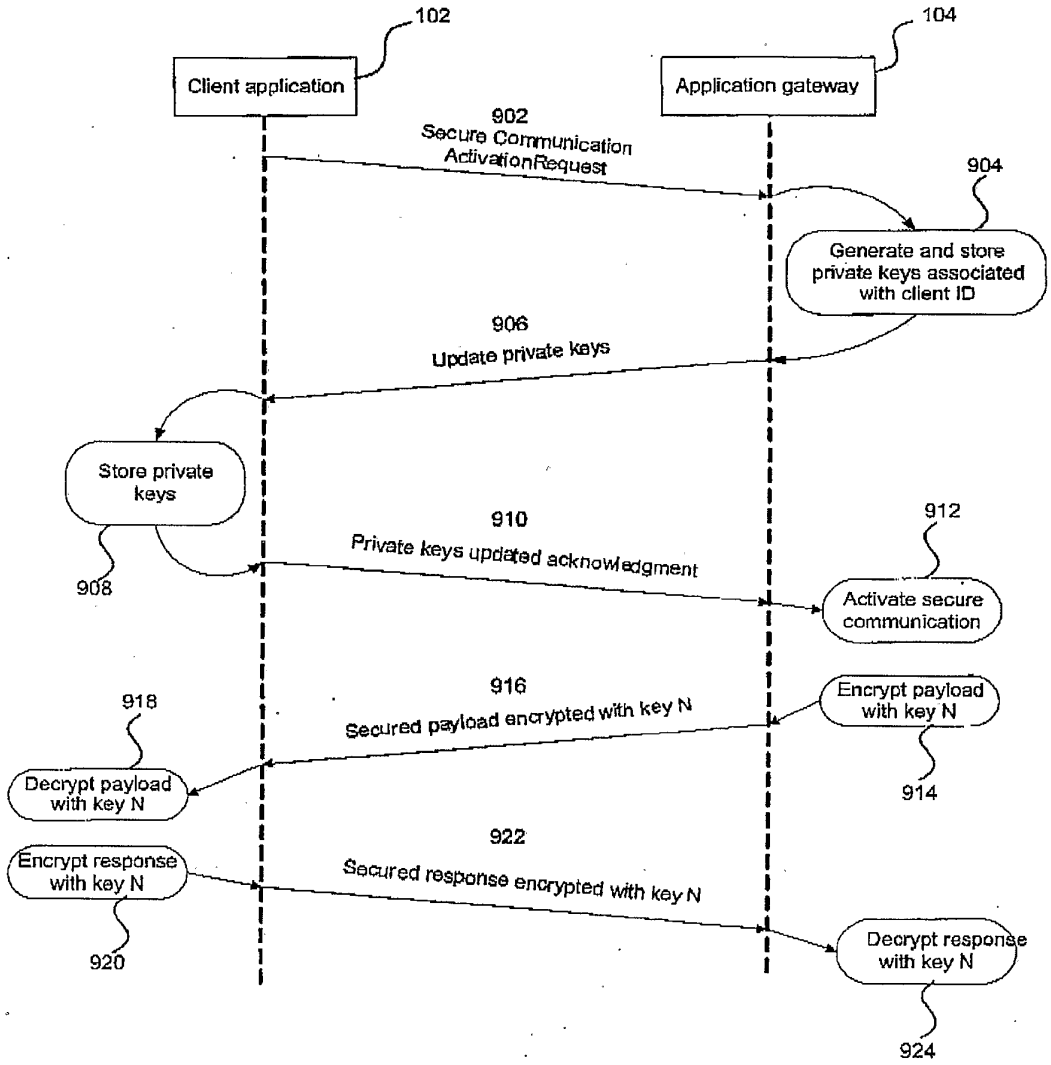

102
Client application
104
Application gateway
902
Secure Communication ActivationRequest
904
Generate and store private keys associated with client ID
906
Update private keys
Store private keys
908
910
Private keys updated acknowledgment
912
Activate secure communication
916
Secured payload encrypted with key N
Encrypt payload with key N
914
918
Decrypt payload with key N
922
Secured response encrypted with key N
Encrypt response with key N
920
Decrypt response with key N
924

FIGURE 10

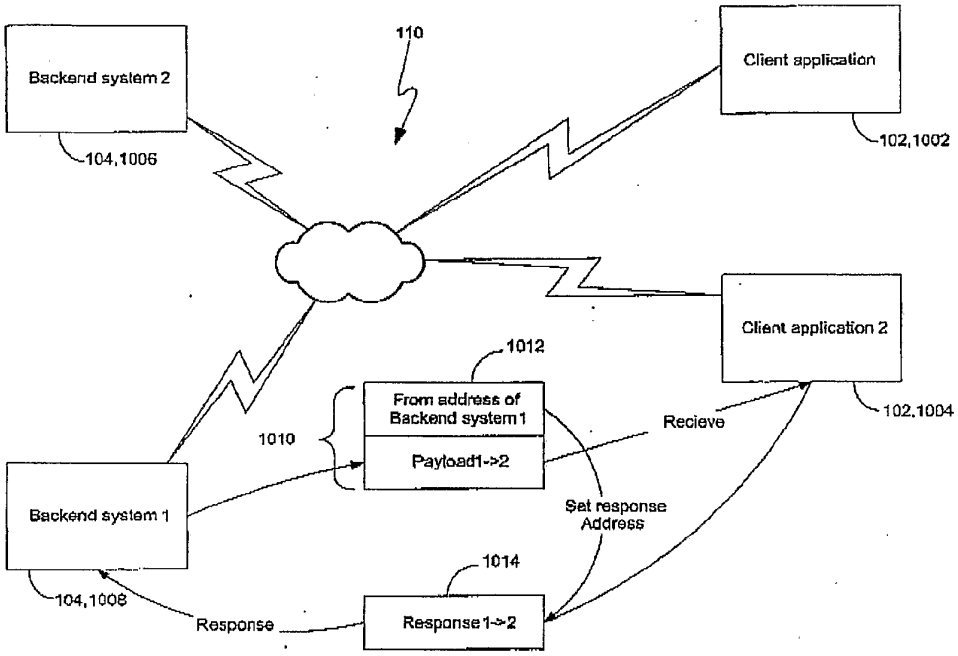

Backend system 2
104,1006
110
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Backend system 1
Set response Address
1014
104,1008
Response
Response 1->2

FIGURE 11

11/31

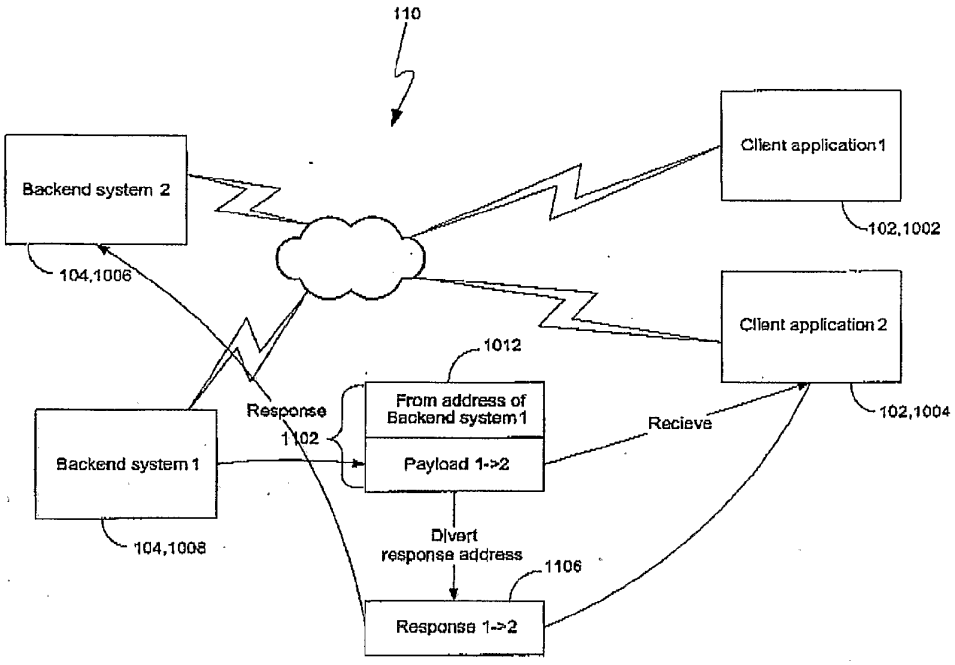


FIGURE 12

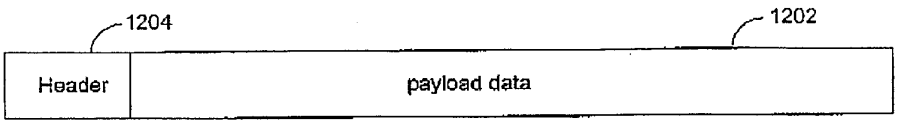


FIGURE 13

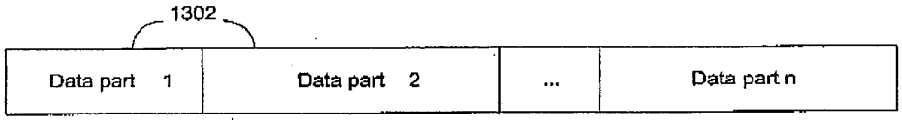


FIGURE 14

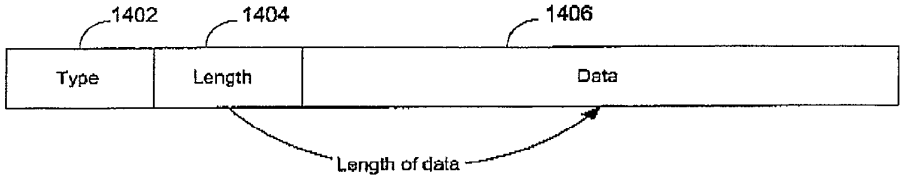


FIGURE 15

Workflow Instruction data structure

	Type	Data
Menu Single/Multiple Select	S,M	[PARAMETER] [TITLE] [ITEM1] [ITEM2] ..... [ITEMn]
Information Message	I	[TITLE] [MESSAGE]
Header Response	H	[HEADER]
Redirect Address	R	[PHONE NUMBER]
User Input	T	[PARAMETER] [LABEL] [TYPE]
Execute URL	E	[URL]
Jump to index	J	[CMD Index]
Go to previous Cmd	P	
Branch menu	B	[PARAMETER] [TITLE] [Label1,index1] [Label2,index2] ..... [ITEMn]
No-op	N	
Store Permanent	K	[Title]
Clear Permanent Storage	D	
Read System Property	p	[Property name]
Configuration Settings	C	[Configurations]

Type enumeration:
TYPE_ANY = 0;
TYPE_EMAILADDR=1;
TYPE_NUMERIC = 2;
TYPE_PHONENUMBER = 3;
TYPE_URL = 4;
TYPE_DECIMAL = 5;

FIGURE 16

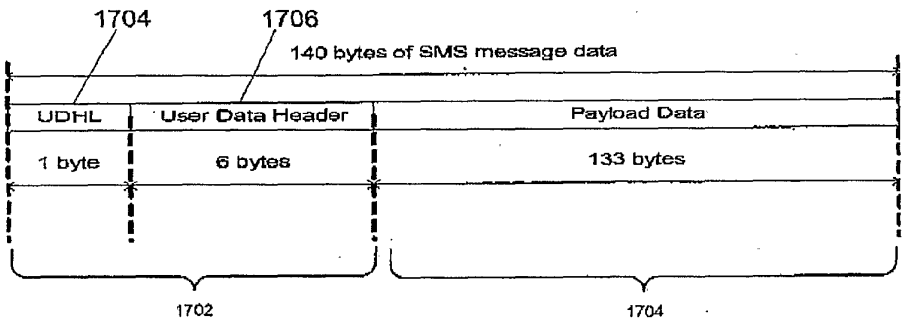

1704
1706
140 bytes of SMS message data
UDHL
User Data Header
Payload Data
1 byte
6 bytes
133 bytes
1702
1704

FIGURE 17

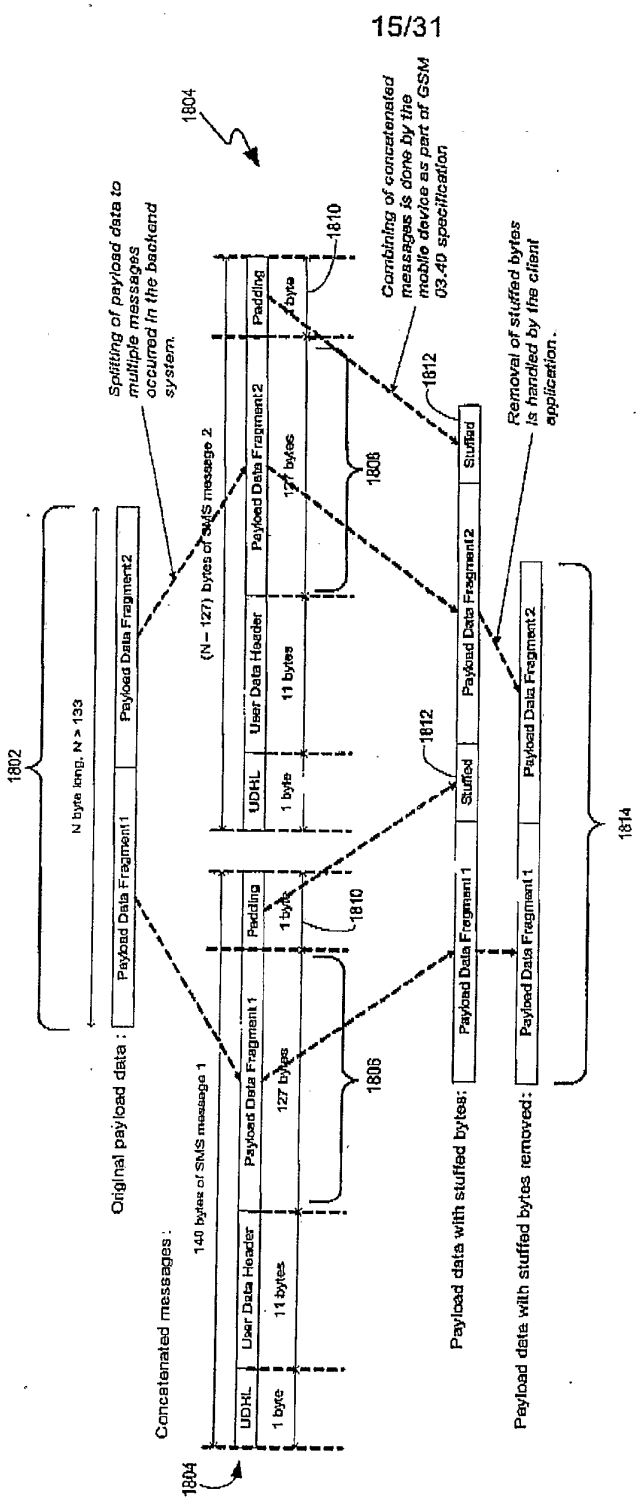

1804
Splitting of payload data to multiple messages occured in the backend system.
Combining of concatenated messages is done by the mobile device as part of GSM 03.40 specification
Removal of stuffed bytes is handled by the client application.
1802
N byte long, N > 133
Original payload data :
Payload Data Fragment 1
Payload Data Fragment2
(N – 127) bytes of SMS message 2
UDHL
User Data Header
Payload Data Fragment2
Padding
1 byte
11 bytes
127 bytes
1 byte
1810
1808
1812
Stuffed
Payload data with stuffed bytes:
Payload data with stuffed bytes removed:
1806
140 bytes of SMS message 1
Concatenated messages :
1814

FIGURE 18

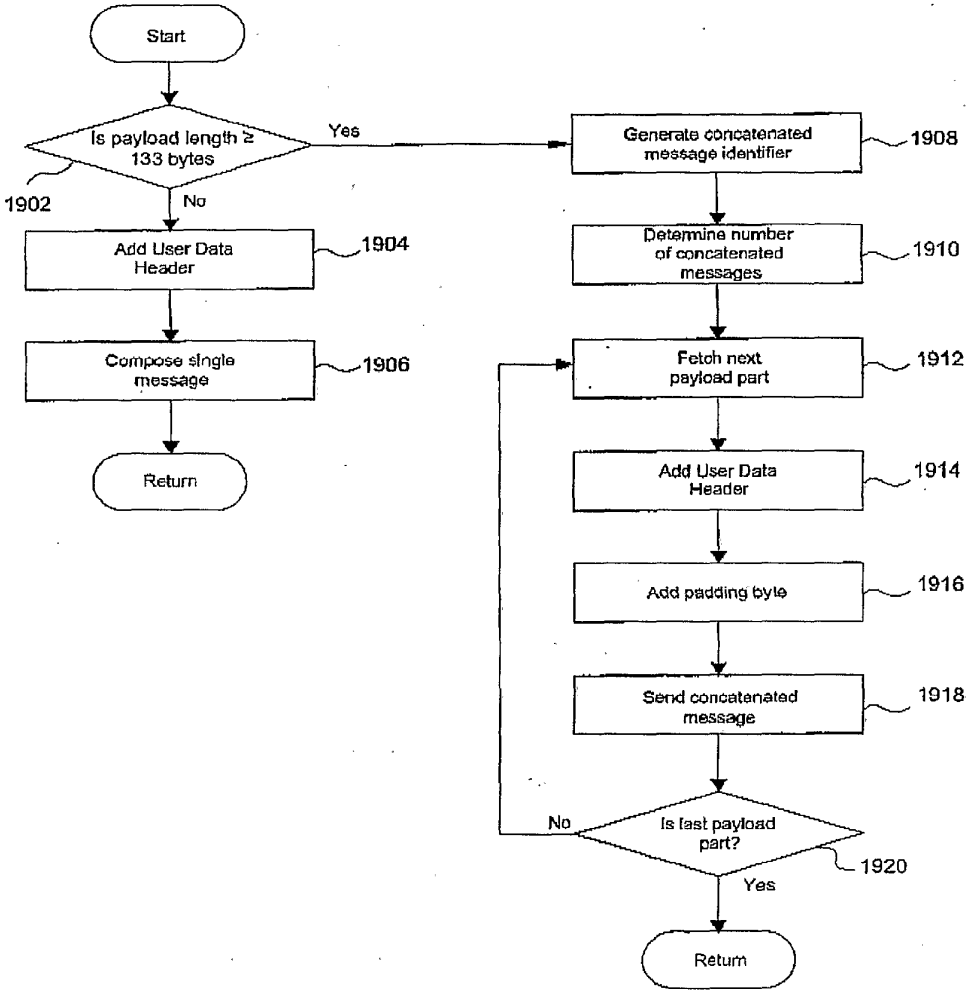

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
No
Yes
1920
Return

FIGURE 19

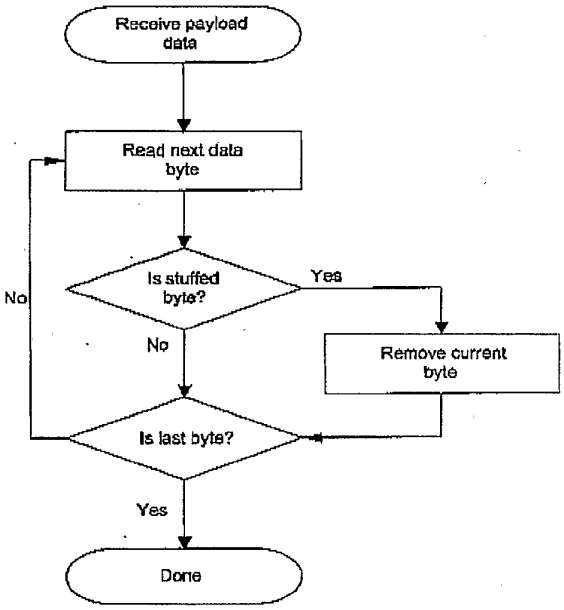

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
No
Is last byte?
Yes
Done

FIGURE 20

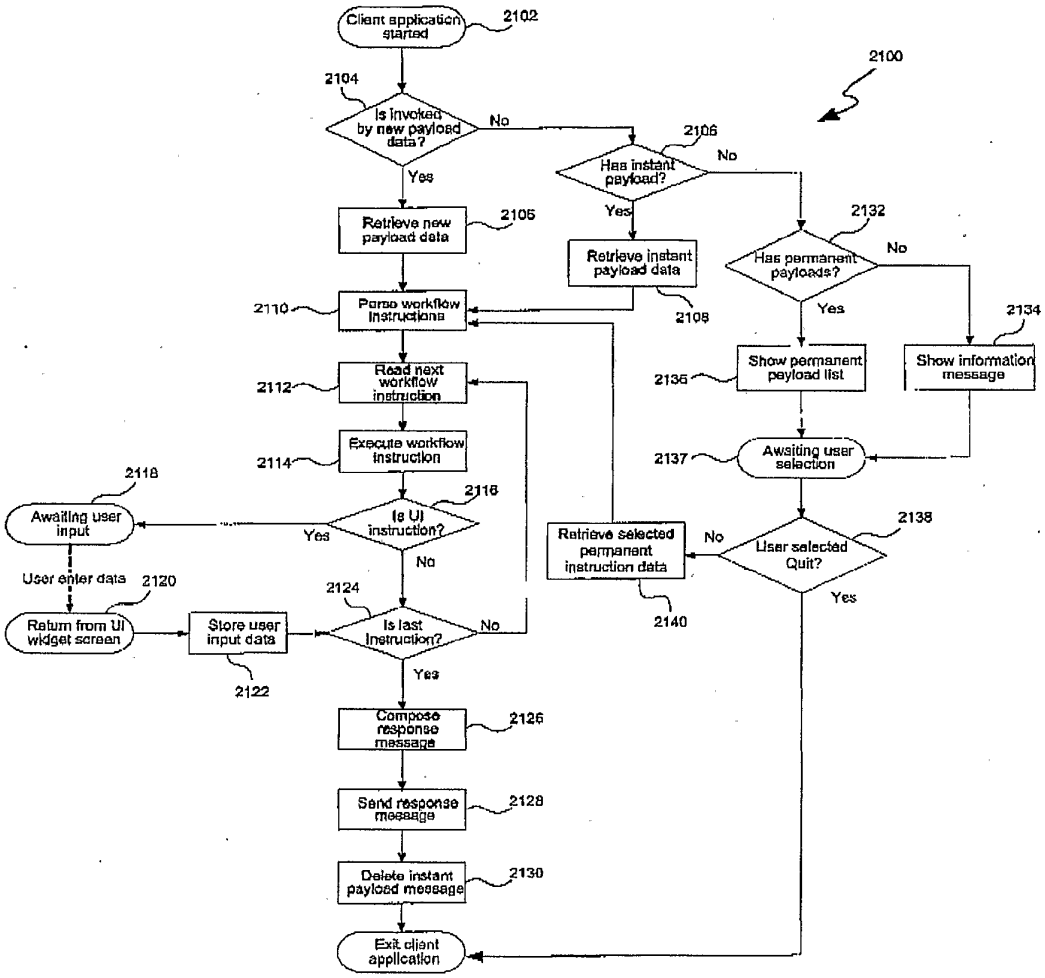

Client application started
2102
2100
2104
Is invoked by new payload data?
No
2106
Has instant payload?
No
Yes
Yes
Retrieve new payload data
2105
Retrieve instant payload data
2108
2132
Has permanent payloads?
No
Yes
2134
2110
Parse workflow instructions
2136
Show permanent payload list
Show information message
2112
Read next workflow instruction
2114
Execute workflow instruction
2137
Awaiting user selection
2118
Awaiting user input
2116
Is UI instruction?
Yes
No
2138
User selected Quit?
No
Yes
Retrieve selected permanent instruction data
2140
User enter data
2120
Return from UI widget screen
Store user input data
2122
2124
Is last instruction?
No
Yes
2126
Compose response message
2128
Send response message
2130
Delete instant payload message
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

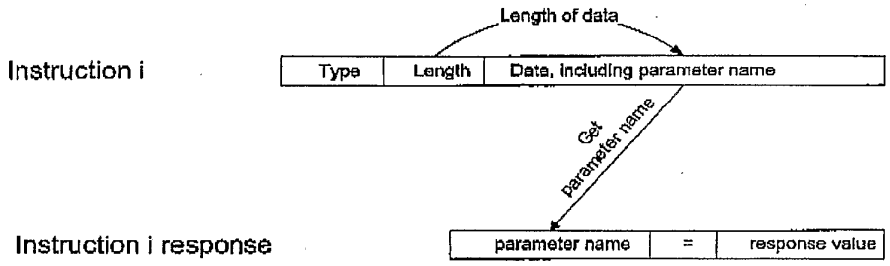


FIGURE 23

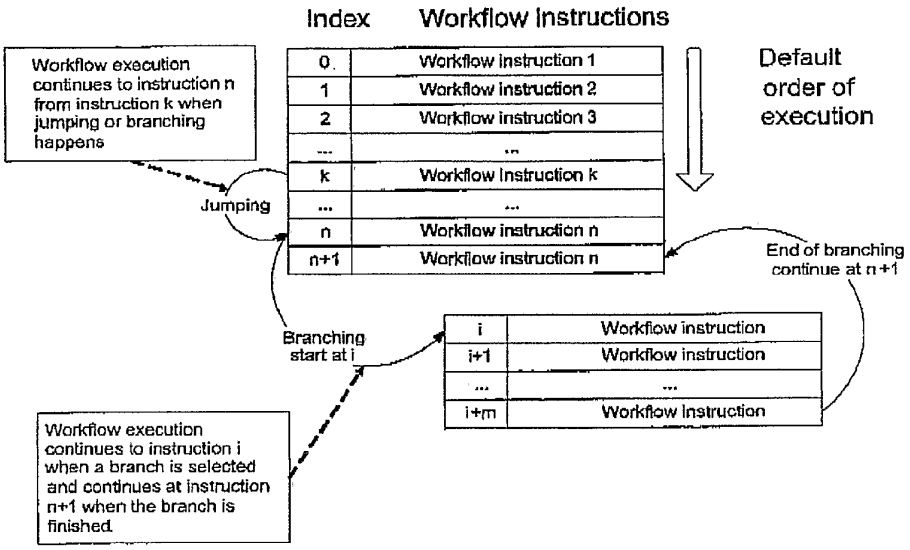

Index
Workflow Instructions
Default order of execution
Workflow execution continues to instruction n from instruction k when jumping or branching happens
Jumping
0
Workflow instruction 1
1
Workflow instruction 2
2
Workflow instruction 3
k
Workflow instruction k
n
Workflow instruction n
n+1
Workflow instruction n
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished

FIGURE 24

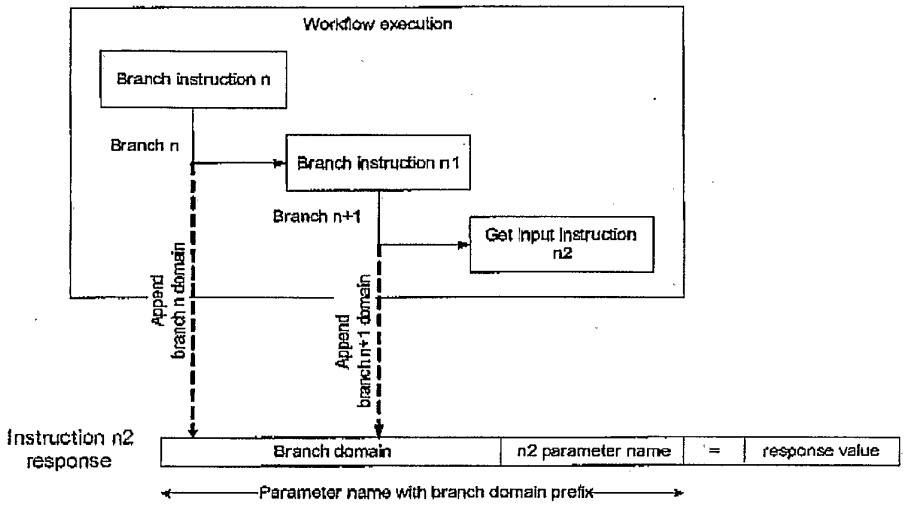

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get Input Instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

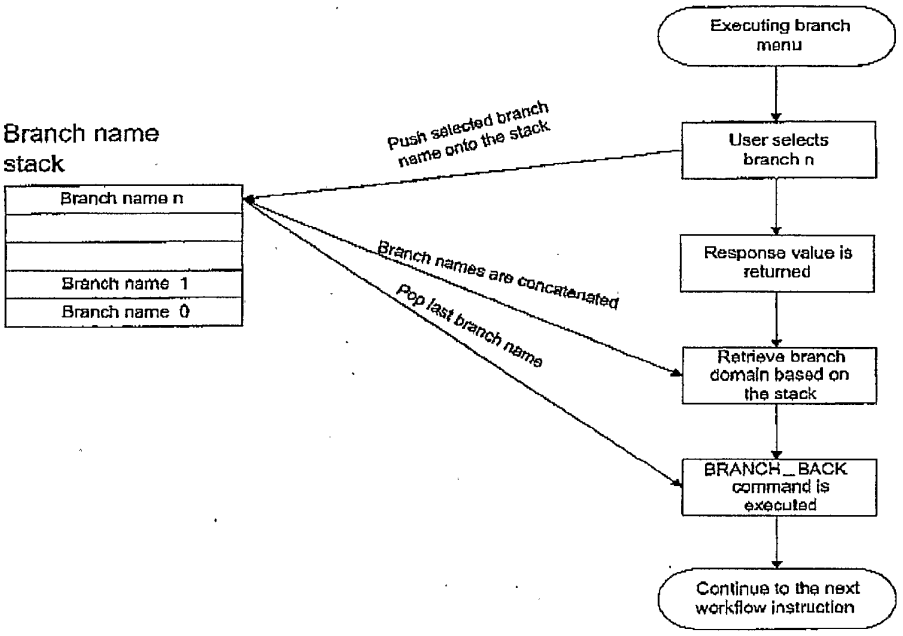

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name
Branch name stack
Branch name n
Branch name 1
Branch name 0

FIGURE 26

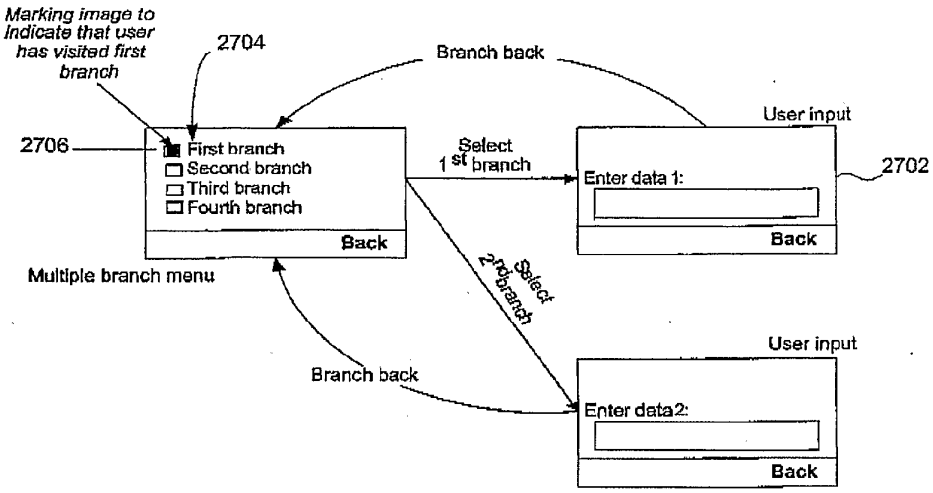


FIGURE 27

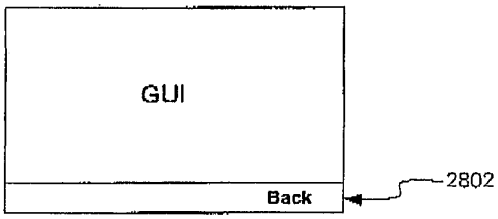


FIGURE 28

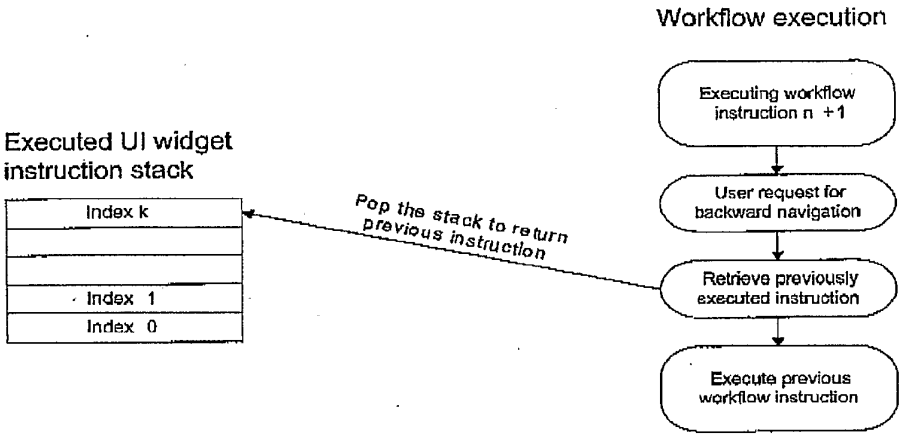

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

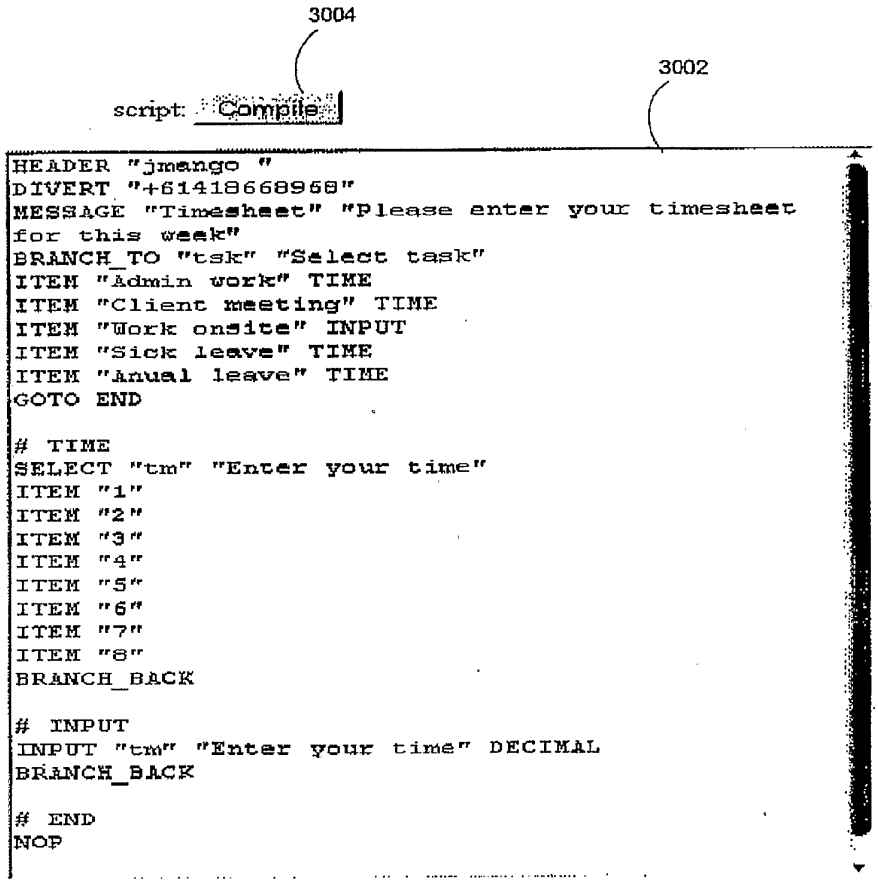

3004
3002
script:
Compile
HEADER "jmango "
DIVERT "+61418668968"
MESSAGE "Timesheet" "Please enter your timesheet
for this week"
BRANCH_TO "tsk" "Select task"
ITEM "Admin work" TIME
ITEM "Client meeting" TIME
ITEM "Work onsite" INPUT
ITEM "Sick leave" TIME
ITEM "Anual leave" TIME
GOTO END
TIME
SELECT "tm" "Enter your time"
ITEM "1"
ITEM "2"
ITEM "3"
ITEM "4"
ITEM "5"
ITEM "6"
ITEM "7"
ITEM "8"
BRANCH_BACK
INPUT
INPUT "tm" "Enter your time" DECIMAL
BRANCH_BACK
END
NOP

FIGURE 30

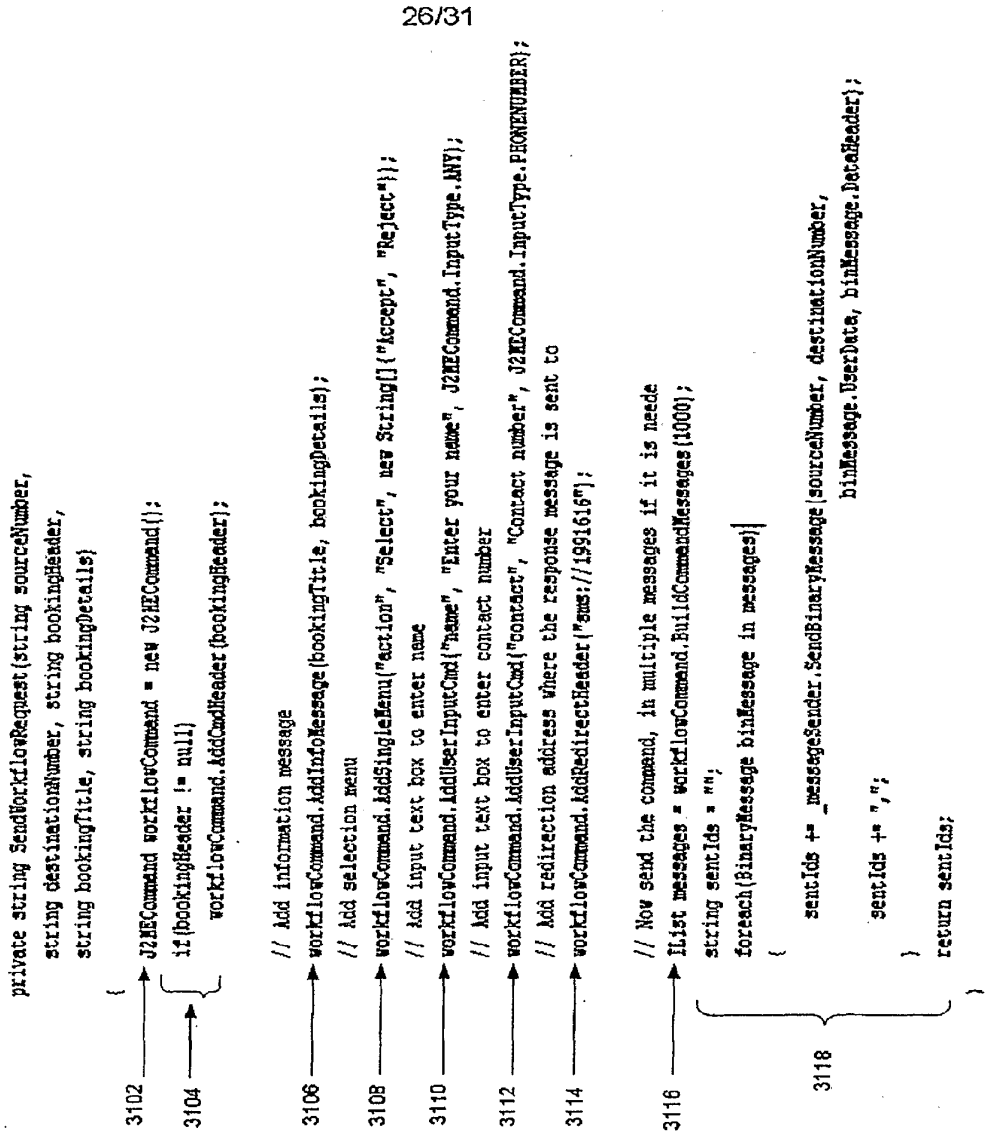

private string SendWorkflowRequest(string sourceNumber,
string destinationNumber, string bookingHeader,
string bookingTitle, string bookingDetails)
{
3102
J2MECommand workflowCommand = new J2MECommand();
3104
if(bookingHeader != null)
workflowCommand.AddCmdHeader(bookingHeader);
// Add information message
3106
workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
// Add selection menu
3108
workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
// Add input text box to enter name
3110
workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
// Add input text box to enter contact number
3112
workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
// Add redirection address where the response message is sent to
3114
workflowCommand.AddRedirectHeader("sms://199161");
// Now send the command, in multiple messages if it is neede
3116
Hist messages = workflowCommand.BuildCommandMessages(1000);
string sentIds = "";
foreach(BinaryMessage binMessage in messages)
{
3118
sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
binMessage.UserData, binMessage.DataHeader);
sentIds += ",";
}
return sentIds;
}

FIGURE 31

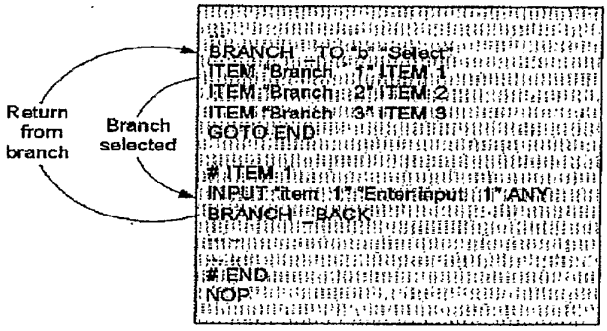


FIGURE 32

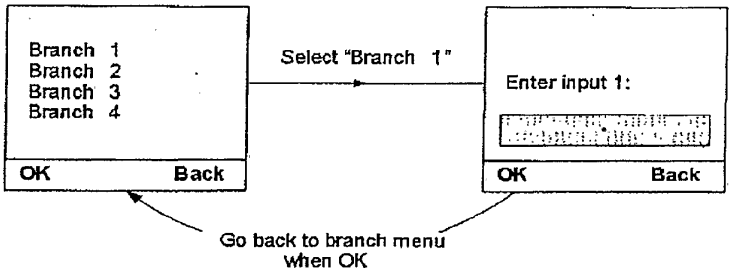


FIGURE 33

28/31

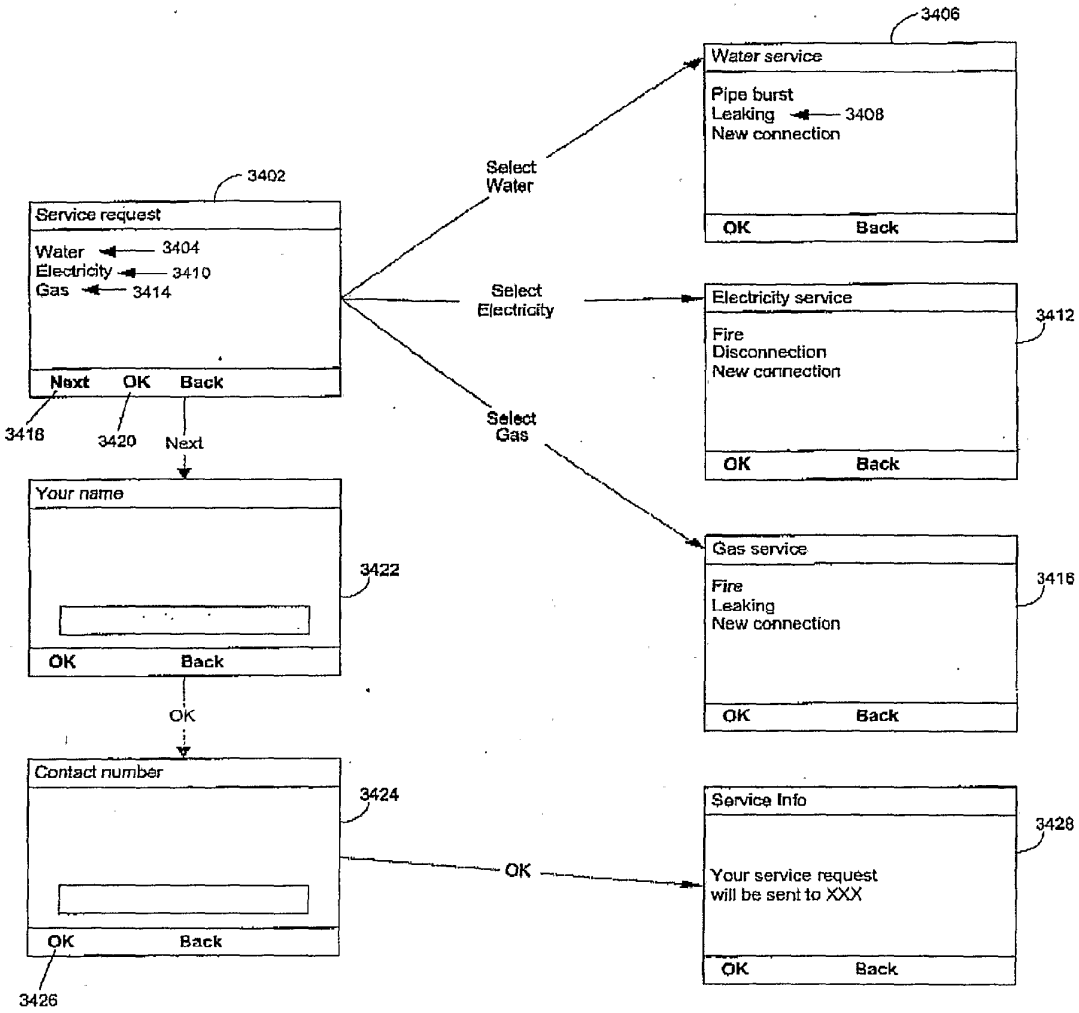


FIGURE 34

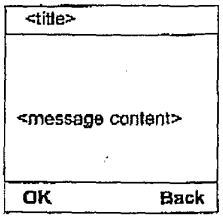


FIGURE 35

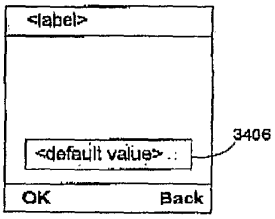


FIGURE 36

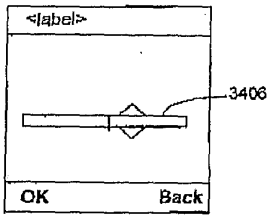


FIGURE 37

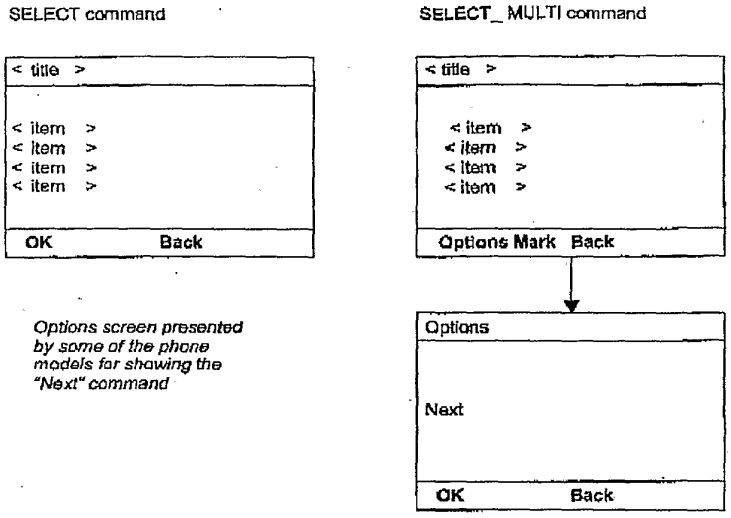

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

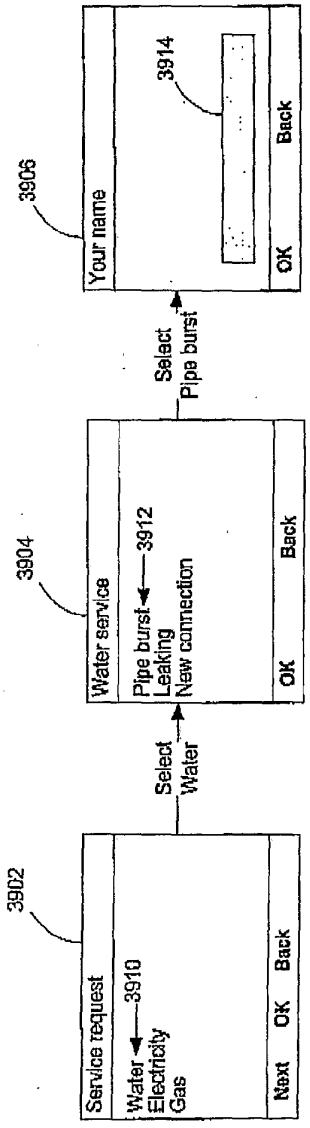
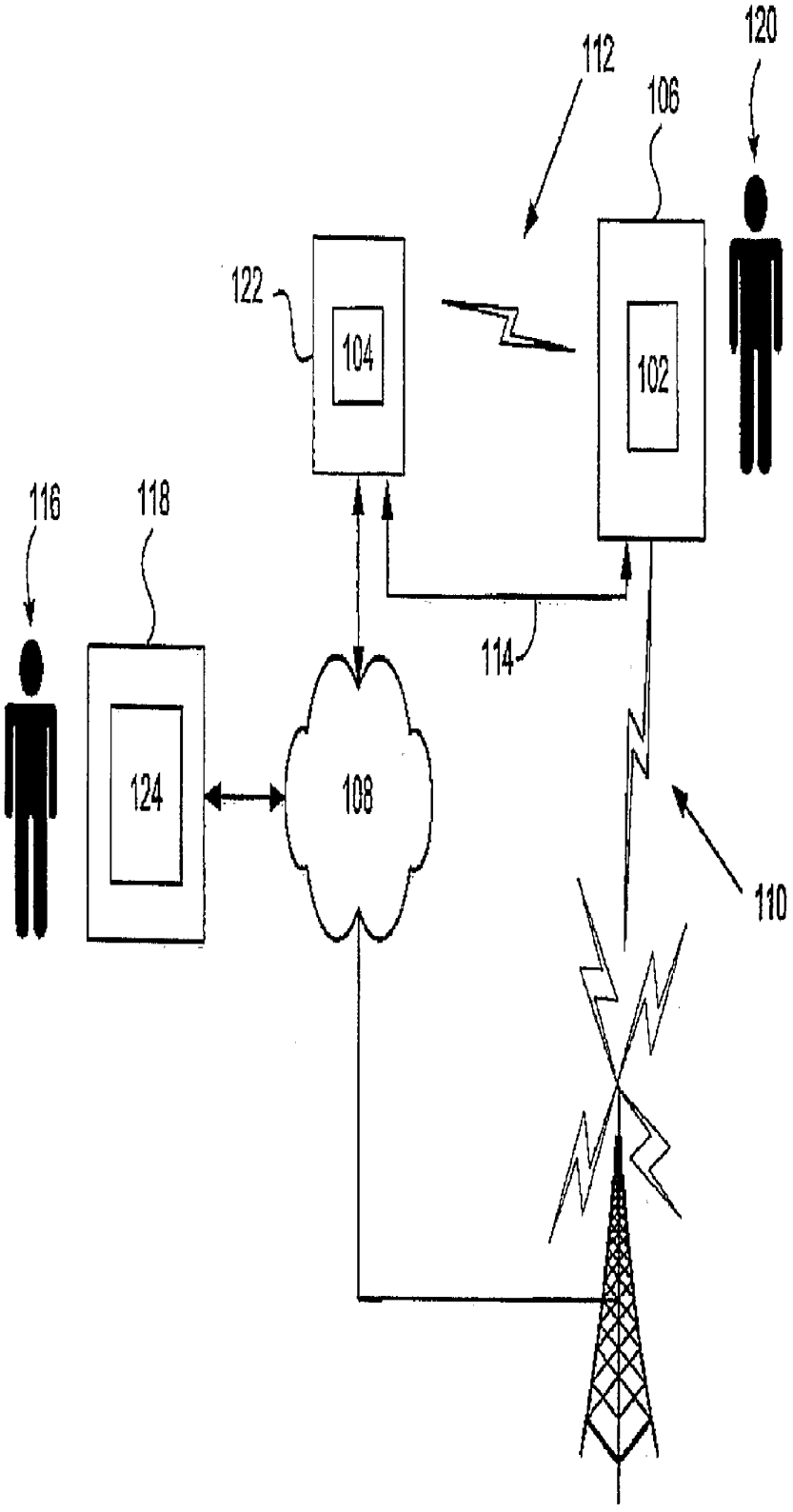

3902
Service request
Water
Electricity
Gas
3910
Next
OK
Back
Select
Water
3904
Water service
Pipe burst
Leaking
New connection
3912
OK
Back
Select
Pipe burst
3906
Your name
3914
OK
Back

FIGURE 39


112
120
106
122
104
102
116
118
114
124
108
110

Espacenet

Bibliographic data: CN101606400 (A) — 2009-12-16

An interactive system and process

Inventor(s): ANH NGO DUC [AU] ± (NGO DUC ANH)

Applicant(s): DELOITTE SERVICES PTY LTD [AU] ± (DELOITTE SERVICES PTY LTD)

Classification: - international: ***H04W4/14; H04W4/18; H04W8/24***
- Euro: G06F8/65; H04M3/42E5; H04W8/24N

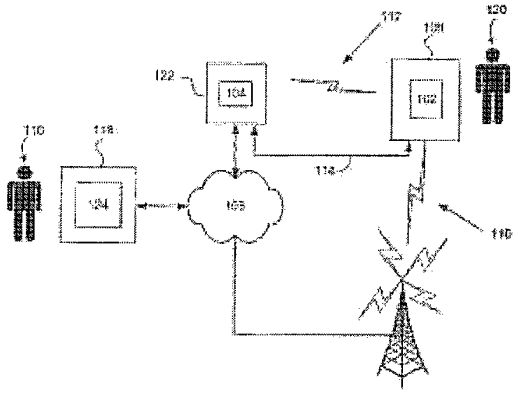
Application number: CN20078038721 20071019

Priority number (s): AU20060905829 20061019

Also published as: WO2008046161 (A1) US2010197326 (A1) EP2084921 (A1) CA2666616 (A1) AU2007312879 (A1) more

Abstract of CN101606400 (A)

A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).



Espacenet

Bibliographic data: CN102073958 (A) — 2011-05-25

System and method for implementing mobile payment

Inventor(s): KAI WEI; CHENJIE YU; TIANXIA FU ± (WEI KAI, ; YU CHENJIE, ; FU TIANXIA)

Applicant(s): TIANJIN ZTE SOFTWARE CORP ± (TIANJIN ZTE SOFTWARE CORPORATION)

Classification: - international: ***G06Q30/00; G07G1/14; H04L29/06; H04W88/02***
- European:

Application number: CN20091228730 20091125

Priority number(s): CN20091228730 20091125

Abstract of CN102073958 (A)

The invention provides a system and a method for implementing mobile payment. The method comprises that: when the transaction type is online account, a management information system (MIS) merchant device acquires transaction data of a mobile payment terminal and personal identification codes of a user, encrypts the personal identification codes, and packs the encrypted personal identification codes, the transaction data and point of sale (POS) terminal information into 8583 online transaction message together; after receiving the 8583 online transaction message, a mobile payment platform judges whether the transaction request is valid, if so, verifies the validities of the user and the account and verifies the personal identification codes; if the user and the account are valid and the personal identification codes are correct, accounting treatment of the transaction is completed; and the mobile payment terminal is a mobile terminal with a radio frequency-subscriber identity module (RF-SIM) card. By adopting the technical scheme of the invention, noncontact mobile payment can be quickly, effectively and securely implemented.

Last updated: 24.09.2012 Worldwide Database 5.7.42; 93p

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102073958 A
(43)申请公布日 2011.05.25

(21)申请号 200910228730.6

(22)申请日 2009.11.25

(71)申请人 天津中兴软件有限责任公司
地址 300300 天津市空港物流加工区中环西路与西三道交口万顺大厦4座

(72)发明人 魏凯 于晨捷 傅天侠

(51)Int.Cl.
G06Q 30/00(2006.01)
G07G 1/14(2006.01)
H04L 29/06(2006.01)
H04W 88/02(2009.01)

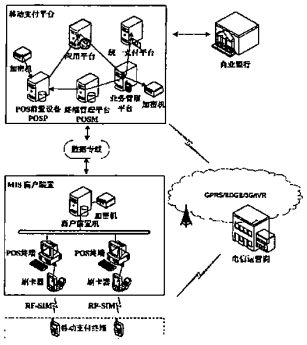
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

一种实现移动支付的系统及方法

(57)摘要

本发明提供一种实现移动支付的系统及方法，该方法包括，当交易类型为在线账户时，MIS商户装置获取移动支付终端的交易数据以及用户的个人识别码，并将个人识别码加密后连同所述交易数据、POS终端信息一起封装成8583联机交易报文；移动支付平台收到8583联机交易报文后判断交易请求是否合法，若交易请求合法则验证用户及账户的合法性，以及对个人识别码进行验证，若用户及账户合法，且个人识别码正确则完成本次交易的账务处理；移动支付终端为具有RF-SIM卡的移动终端。采用本发明的技术方案，可快速、有效、安全地实现非接触式移动支付。



CN 102073958 A

1. 一种实现移动支付的方法，包括：当交易类型为在线账户时，MIS 商户装置获取移动支付终端的交易数据以及用户的个人识别码，并将所述个人识别码加密后连同所述交易数据、POS 终端信息一起封装成 8583 联机交易报文；

所述移动支付平台收到所述 8583 联机交易报文后判断交易请求是否合法，若交易请求合法则验证用户及账户的合法性，以及对所述个人识别码进行验证，若用户及账户合法，且个人识别码正确则完成本次交易的账务处理；

所述移动支付终端为具有 RF-SIM 卡的移动终端。

2. 如权利要求 1 所述的方法，其特征在于：

所述 MIS 商户装置还对 8583 联机交易报文进行 MAC 生成后发送至对应的移动支付平台；

所述移动支付平台收到所述 8583 联机交易报文后先进行 MAC 验证，若 MAC 验证通过再进行所述用户及账户的合法性验证。

3. 如权利要求 1 或 2 所述的方法，其特征在于：

位于移动支付平台的 POS 前置设备收到所述 8583 联机交易报文后，于 MAC 验证通过后对所述个人识别码进行转加密，然后将报文转换为类 8583 报文通过应用平台发送至业务管理平台；

所述对个人识别码进行验证是指，对被加密的个人识别码进行解密，若解密后的个人识别码与本地存储的个人识别码一致则验证通过，否则验证未通过。

4. 如权利要求 2 所述的方法，其特征在于：

所述 MIS 商户装置还存储 POS 终端与 POS 前置设备的对应关系，MIS 商户装置根据所述 POS 终端信息查找该对应关系后确定处理本次交易的 POS 前置设备。

5. 如权利要求 3 所述的方法，其特征在于：

所述 MIS 商户装置对个人识别码进行加密的 PIK1 由 POS 前置设备产生，所述 POS 前置设备对个人识别码进行转加密的 PIK2 由业务管理平台产生；

进行 MAC 验证的 MAK 是由 POS 前置设备产生，各网元的 MAK 一致；

PIK1、PIK2 及各网元处的 MAK 均被 KEK 加密后存储，但各网元处的 KEK 不同。

6. 一种实现移动支付的方法，包括：当交易类型为现金账户时，MIS 商户装置获取移动支付终端的交易数据及移动支付终端的余额信息后，验证本次交易是否合法以及所述移动支付终端的现金账户余额是否足够本次交易，若交易合法且现金账户余额足够本次交易，则完成本次离线交易处理；所述移动支付终端为具有 RF-SIM 卡的移动终端。

7. 一种实现移动支付的系统，包括：移动支付终端、MIS 商户装置及移动支付平台；其特征在于：

所述移动支付终端为具有 RF-SIM 卡的移动终端；

所述 MIS 商户装置用于当交易类型为在线账户时获取交易数据以及用户的个人识别码，并将加密后的个人识别码连同所述交易数据、POS 终端信息一起封装成 8583 联机交易报文后发送至移动支付平台；

所述移动支付平台用于收到所述 8583 联机交易报文后判断交易请求是否合法，若交易请求合法则验证用户及账户的合法性，以及对所述个人识别码进行验证，还用于用户及账户合法，且个人识别码正确时完成本次交易的账务处理。

APPL-1002
APPLE INC. / Page 367 of 1892

8. 如权利要求 7 所述的系统，其特征在于：

所述移动支付平台包括 POS 前置设备、应用平台及业务管理平台；

所述 MIS 商户装置还用于对所述 8583 联机交易报文加封装企业代码后进行 MAC 生成，并将所述 8583 联机交易报文发送至 POS 前置设备；

所述 POS 前置设备用于对所述 8583 联机交易报文进行 MAC 验证，并于 MAC 验证通过后判断交易请求是否合法，若合法则将所述 8583 联机交易报文转换为类 8583 报文后进行 MAC 生成，之后发送至对应的应用平台；

所述应用平台用于收到所述类 8583 报文后进行 MAC 验证，以及 MAC 验证通过后验证用户及账户的合法性，还用于当用户及账户合法后对所述类 8583 报文进行 MAC 生成后发送至业务管理平台；

所述业务管理平台用于收到所述报文后对所述类 8583 报文进行 MAC 验证，以及 MAC 验证通过后对所述个人识别码进行验证，若个人识别码正确则完成本次交易的账务处理。

9. 如权利要求 7 或 8 所述的系统，其特征在于：

所述 POS 前置设备还用于收到所述 8583 联机交易报文后对所述个人识别码进行转加密，以及将转加密后的个人识别码连同所述交易数据、本 POS 终端信息一起封装成类 8583 报文；

所述业务管理平台对个人识别码进行验证是指，业务管理平台对加密后的个人识别码进行解密，若解密后的个人识别码与本地存储的个人识别码一致则验证通过，否则验证未通过。

10. 如权利要求 7 所述的系统，其特征在于：

所述商户端前置机还用于存储各 POS 终端与 POS 前置设备对应关系的路由信息，以及根据 POS 终端信息查询本地存储的路由信息，确定处理该交易报文的 POS 前置设备，并将交易报文发送至对应的 POS 前置设备。

11. 如权利要求 9 所述的系统，其特征在于：

所述 POS 前置设备还用于产生对个人识别码进行加密的 PIK1，并将其发送至 MIS 商户装置；

所述业务管理平台还用于对个人识别码进行转加密的 PIK2，并将其发送至 POS 前置设备；

所述 PIK1、PIK2 及各网元处的 MAK 均被 KEK 加密后存储，但各网元处的 KEK 不同。

12. 一种实现移动支付的系统，包括：移动支付终端及 MIS 商户装置；其特征在于：

所述移动支付终端为具有 RF-SIM 卡的移动终端；

所述 MIS 商户装置用于当交易类型为现金账户时获取交易数据及移动支付终端的余额信息，还用于验证本次交易是否合法以及所述移动支付终端的现金账户余额是否足够本次交易，若交易合法且现金账户余额足够本次交易，则完成本次离线交易处理。

APPL-1002
APPLE INC. / Page 368 of 1892

一种实现移动支付的系统及方法

技术领域

[0001] 本发明涉及电子支付及金融领域，具体涉及一种实现移动支付的系统及方法。

背景技术

[0002] 移动支付论坛 (Mobile Payment Forum) 认为："移动支付是指进行交易的双方，以一定信用额度或一定金额的存款，为了某种货物或者业务，通过移动设备从移动支付商处兑换到代表相同金额的数据，以移动终端为媒介将该数据转移给支付对象，从而清偿消费费用进行商业交易的支付方式。"

[0003] 按实现方式和距离，移动支付可分为两种：一种是远程支付。以银行账户、手机话费或虚拟预存储账户作为支付账户，以短信、语音、WAP 等方式提起业务请求。第二种是现场支付。通过近距离非接触无线通信技术，如红外技术、RFID 射频识别技术、NFC(Near Field Communication，近距离无线通讯）技术、蓝牙技术等，在手机终端和 POS(Point Of Sale，销售点终端）机、自动售货机、售票机等设备之间进行支付信息的交换，真正实现用手机完成面对面的支付交易。

发明内容

[0004] 本发明要解决的技术问题是提供一种实现移动支付的系统及方法，可快速、有效、安全地实现非接触式移动支付。

[0005] 为了解决上述问题，本发明提供了一种实现移动支付的方法，包括：当交易类型为在线账户时，MIS 商户装置获取移动支付终端的交易数据以及用户的个人识别码，并将所述个人识别码加密后连同所述交易数据、POS 终端信息一起封装成 8583 联机交易报文；

[0006] 所述移动支付平台收到所述 8583 联机交易报文后判断交易请求是否合法，若交易请求合法则验证用户及账户的合法性，以及对所述个人识别码进行验证，若用户及账户合法，且个人识别码正确则完成本次交易的账务处理；

[0007] 所述移动支付终端为具有 RF-SIM 卡的移动终端。

[0008] 进一步地，所述 MIS 商户装置还对 8583 联机交易报文进行 MAC 生成后发送至对应的移动支付平台；

[0009] 所述移动支付平台收到所述 8583 联机交易报文后先进行 MAC 验证，若 MAC 验证通过再进行所述用户及账户的合法性验证。

[0010] 进一步地，位于移动支付平台的 POS 前置设备收到所述 8583 联机交易报文后，于 MAC 验证通过后对所述个人识别码进行转加密，然后将报文转换为类 8583 报文通过应用平台发送至业务管理平台；

[0011] 所述对个人识别码进行验证是指，对被加密的个人识别码进行解密，若解密后的个人识别码与本地存储的个人识别码一致则验证通过，否则验证未通过。

[0012] 进一步地，所述 MIS 商户装置还存储 POS 终端与 POS 前置设备的对应关系，MIS 商户装置根据所述 POS 终端信息查找该对应关系后确定处理本次交易的 POS 前置设备。

APPL-1002
APPLE INC. / Page 369 of 1892

[0013] 进一步地，所述 MIS 商户装置对个人识别码进行加密的 PIK1 由 POS 前置设备产生，所述 POS 前置设备对个人识别码进行转加密的 PIK2 由业务管理平台产生；

[0014] 进行 MAC 验证的 MAK 是由 POS 前置设备产生，各网元的 MAK 一致；

[0015] PIK1、PIK2 及各网元处的 MAK 均被 KEK 加密后存储，但各网元处的 KEK 不同。

[0016] 本发明还提供一种实现移动支付的方法，包括：当交易类型为现金账户时，MIS 商户装置获取移动支付终端的交易数据及移动支付终端的余额信息后，验证本次交易是否合法以及所述移动支付终端的现金账户余额是否足够本次交易，若交易合法且现金账户余额足够本次交易，则完成本次离线交易处理；所述移动支付终端为具有 RF-SIM 卡的移动终端。

[0017] 本发明还提供一种实现移动支付的系统，包括：移动支付终端、MIS 商户装置及移动支付平台；

[0018] 所述移动支付终端为具有 RF-SIM 卡的移动终端；

[0019] 所述 MIS 商户装置用于当交易类型为在线账户时获取交易数据以及用户的个人识别码，并将加密后的个人识别码连同所述交易数据、POS 终端信息一起封装成 8583 联机交易报文后发送至移动支付平台；

[0020] 所述移动支付平台用于收到所述 8583 联机交易报文后判断交易请求是否合法，若交易请求合法则验证用户及账户的合法性，以及对所述个人识别码进行验证，还用于用户及账户合法，且个人识别码正确时完成本次交易的账务处理。

[0021] 进一步地，所述移动支付平台包括 POS 前置设备、应用平台及业务管理平台；

[0022] 所述 MIS 商户装置还用于对所述 8583 联机交易报文加封装企业代码后进行 MAC 生成，并将所述 8583 联机交易报文发送至 POS 前置设备；

[0023] 所述 POS 前置设备用于对所述 8583 联机交易报文进行 MAC 验证，并于 MAC 验证通过后判断交易请求是否合法，若合法则将所述 8583 联机交易报文转换为类 8583 报文后进行 MAC 生成，之后发送至对应的应用平台；

[0024] 所述应用平台用于收到所述类 8583 报文后进行 MAC 验证，以及 MAC 验证通过后验证用户及账户的合法性，还用于当用户及账户合法后对所述类 8583 报文进行 MAC 生成后发送至业务管理平台；

[0025] 所述业务管理平台用于收到所述报文后对所述类 8583 报文进行 MAC 验证，以及 MAC 验证通过后对所述个人识别码进行验证，若个人识别码正确则完成本次交易的账务处理。

[0026] 进一步地，所述 POS 前置设备还用于收到所述 8583 联机交易报文后对所述个人识别码进行转加密，以及将转加密后的个人识别码连同所述交易数据、本 POS 终端信息一起封装成类 8583 报文；

[0027] 所述业务管理平台对个人识别码进行验证是指，业务管理平台对加密后的个人识别码进行解密，若解密后的个人识别码与本地存储的个人识别码一致则验证通过，否则验证未通过。

[0028] 进一步地，所述商户端前置机还用于存储各 POS 终端与 POS 前置设备对应关系的路由信息，以及根据 POS 终端信息查询本地存储的路由信息，确定处理该交易报文的 POS 前置设备，并将交易报文发送至对应的 POS 前置设备。

APPL-1002
APPLE INC. / Page 370 of 1892

[0029] 进一步地，所述 POS 前置设备还用于产生对个人识别码进行加密的 PIK1，并将其发送至 MIS 商户装置；

[0030] 所述业务管理平台还用于对个人识别码进行转加密的 PIK2，并将其发送至 POS 前置设备；

[0031] 所述 PIK1、PIK2 及各网元处的 MAK 均被 KEK 加密后存储，但各网元处的 KEK 不同。

[0032] 本发明还提供一种实现移动支付的系统，包括：移动支付终端及 MIS 商户装置；

[0033] 所述移动支付终端为具有 RF-SIM 卡的移动终端；

[0034] 所述 MIS 商户装置用于当交易类型为现金账户时获取交易数据及移动支付终端的余额信息，还用于验证本次交易是否合法以及所述移动支付终端的现金账户余额是否足够本次交易，若交易合法且现金账户余额足够本次交易，则完成本次离线交易处理。

[0035] 本发明所基于的 RF-SIM 技术，即是现场支付技术的一种，它通过将射频技术集成到手机 SIM 卡里，使手机使用者仅需要更换一张智能卡，便可以使现有的手机变成类 NFC 手机，不但拥有普通 SIM 卡的所有功能，还拥有一个可代替钱包、钥匙和身份证的全方位服务平台。其中 SIM 卡部分用于正常的手机移动通讯、鉴权，仅用作与手机的物理连接。内置软件用于管理高安全度的 RF-ID、内置 e-credit 电子信用卡、EMV 电子钱包以及其他基于 mifare 逻辑的 VIP 会员卡。同时使用微型 RF 模块并通过内置的天线与外部设备通讯。

附图说明

[0036] 图 1 是本发明的移动支付系统集中式组网结构图；

[0037] 图 2 是本发明的联机交易流程图；

[0038] 图 3 是本发明的支付账户在线充值流程图；

[0039] 图 4 是本发明的密钥分配体系图。

具体实施方式

[0040] 本发明的主要目的在于提供一种基于 RF-SIM 终端卡技术和 ISO8583 协议的安全高效的电子支付方法，主要用于实现近距离非接触式移动支付。为了兼容现有的银行卡类交易，本发明的交易报文以 ISO8583 规范为基础。在移动支付平台之外，包括 MIS 商户装置和与商业银行的账务接口部分，采用标准 8583 报文；而在移动支付平台之内，则按照系统设计的类 8583 报文进行交易数据的处理和转发。

[0041] 本发明给出了一整套移动支付的解决方案，包括系统架构设计，安全体系建立，以及交易数据传输等。

[0042] 本发明中涉及的几个名词解释如下：

[0043] RF-SIM：RF-SIM 是一种基于 SIM 卡的近 / 中距离无线通信技术，技术支持方为香港直通电讯。此技术是 NFC 近距离无线通信的一种，它将具有 RF 射频功能的模块镶嵌在 SIM 卡内，使用 2.4G 的微波频率进行数据通信。最大特点是用户不需更换手机，是典型的单 SIM 卡移动支付解决方案。

[0044] ISO8583：ISO8583 协议是目前国际上金融系统通用的标准报文协议。它被广泛应用于以银行卡交换为主的金融交易系统，各个银行间通讯，ATM 或 POS 通讯，均采用 ISO8583 报文。目前流行的网银在线、Call Center 与银行之间的通讯报文也是 ISO8583 协议。

APPL-1002
APPLE INC. / Page 371 of 1892

[0045] OTA：是 Over The Air 的缩写，中文称为空中下载。空中下载技术是通过移动通信（GSM 或 CDMA）的空中接口对 SIM 卡数据及应用进行远程管理的技术。空中接口可以采用 WAP、GPRS、CDMA1X 及短消息技术。

[0046] 本发明中实现该方法的系统架构，主要由移动支付终端，MIS 商户装置和移动支付平台三部分组成。这里所指 MIS 商户是指能够受理移动支付业务，所属的 POS 终端通过商户端前置机与移动支付平台相连的零售商、公司或其他机构。

[0047] 如图 1 所示，根据本发明的移动支付系统包括 RF-SIM 移动支付终端，MIS 商户装置和移动支付平台三个主要部分。分别说明如下：

[0048] 移动支付终端：主要是指采用 RF-SIM 技术，可与 POS 终端进行近距离非接触式数据交换的移动终端。还可以通过 OTA 空中下载的方式完成对终端卡的管理，包括对终端卡安全域的划分及通过空中下载方式到业务管理平台下载应用程序；移动支付终端中具有 RF-SIM 卡。

[0049] MIS 商户装置：包括刷卡器，POS 终端和商户前置设备。

[0050] 刷卡器用于当交易类型为现金账户时读取交易数据，并将其发送至 POS 终端，还用于当移动支付终端选择在线账户时获取用户的 PIN（个人识别码），并将 PIN 与交易数据发送至 POS 终端；

[0051] POS 终端用于识别移动支付终端的 RF-SIM 卡参数，包括判断是否支持交易，及本次交易类型（包括在线账户、现金账户等），当交易为现金账户时，移动支付终端的现金账户余额是否足够本次交易；

[0052] POS 终端还用于当交易类型为现金账户时，验证本次交易是否合法，若合法且现金账户余额足够本次交易，则完成本次离线交易处理，包括扣除移动支付终端的现金账户余额。

[0053] POS 终端还用于当交易类型为在线账户时，将收到的 PIN、交易数据连同本 POS 终端信息封装成标准 8583 联机交易报文（该报文包括应用类型标识 AID），并进行 MAC（Message Authentication Code，报文鉴别码）生成后将 8583 联机交易报文发送至商户前置设备。

[0054] POS 终端还用于检查后台系统是否有权限接收 POS 终端的数据；以及数据上传，联机交易处理和信息上传；提供票据打印，出纸错误控制。

[0055] 商户前置设备包括商户前置机和加密机；

[0056] 加密机用于进行密钥转换，即将移动支付平台中的 POS 前置设备发来的经 KEK 加密的 WK（工作密钥，包括 PIK 及 MAK）进行密钥转换后发送给 POS 终端；

[0057] 加密机还用于收到 POS 终端发来的 8583 联机交易报文后进行 MAC 验证，验证通过后再进行 MAC 生成；

[0058] 商户前置机用于将 MAC 生成后的报文加上企业代码等信息后封装成标准 8583 联机交易报文，将交易报文发送至对应的 POS 前置设备。

[0059] 商户前置机还用于存储各 POS 终端与 POS 前置设备对应关系的路由信息，并根据 POS 终端信息查询本地存储的路由信息，从而确定处理该交易报文的 POS 前置设备，并将交易报文发送至对应的 POS 前置设备。

[0060] 移动支付平台包括 POS 前置设备、POS 终端管理平台、应用平台、业务管理平台以

APPL-1002
APPLE INC. / Page 372 of 1892

及统一支付平台，是该移动支付系统的核心部分；其中：

[0061] POS 前置设备，用于生成 WK，并通过 KEK 加密后发送给商户前置机；还用于产生 PIK1，并将其发送至 POS 终端；

[0062] POS 前置设备还用于收到交易报文后进行 MAC 验证，验证通过后对交易报文进行合法性检查，包括终端设备编号及运行状态、操作员、校验位以及 POS 终端的有效期等是否合法，以及交易是否超时、超范围，若合法且未超时、未超范围则使用 PIK2 将 PIN 进行转加密（即重新用 PIK2 对 PIN 进行加密），之后将报文封装成移动支付平台内部通用的类 8583 报文，并根据报文中的 AID 将交易报文转发至对应的应用平台；若交易不合法或交易超时或超范围则拒绝该交易。这样，可以降低应用平台及账务清算平台等的负荷，减少后台系统处理账务所需的开销。

[0063] 应用平台，用于记录移动支付终端对应用程序的下载，如合法下载过哪些应用程序，若移动支付终端曾非法下载过应用程序则将该移动支付终端加入黑名单；还用于收到交易报文后根据黑名单验证用户及账户的合法性，包括该用户是否欠费及是否为黑名单中的用户等，还可以用于按照应用计费原则（如应用的使用次数等）完成相关处理（如为运营商收取一定的手续费），并将报文转发至业务管理平台。

[0064] 应用平台还用于协助业务管理平台完成应用程序的产品测试，以及对应用进行分组，以及提供应用程序的更新，应用的暂停、恢复，以及注销等操作；提供安全控制功能，包括内部操作员管理、移动支付终端交易限制、用户黑名单管理、抽取交易特征及建立风险控制模型等。

[0065] 业务管理平台，用于产生 PIK2，并将其发送至 POS 前置设备；还用于收到交易报文后进行 MAC 验证，MAC 验证通过后对 PIN 进行校验，还用于校验通过后对本次交易进行账务处理，如扣款处理，之后返回交易响应；若校验未通过，则返回交易失败的消息。

[0066] 对 PIN 进行校验是指，用本地存储的 KEK 解密出被加密的 PIK2，之后用 PIK2 解密出报文中的 PIN，然后比较解密出的 PIN 是否与本地存储的 PIN 一致，若一致则校验通过，否则校验未通过；

[0067] 业务管理平台负责用户、商户、SP/CP、支付终端卡片、以及 POS 机的注册和信息管理；提供支付账户的管理功能，包括现金账户（如扣除现金余额）、在线账户（如修改在线账户信息）和积分账户（如修改用户积分等）；提供业务信息的查询统计、分析功能；提供密钥安全管理、应用程序下载。

[0068] POS 终端管理平台主要负责 POS 终端的信息和参数管理；提供 POS 终端应用程序的增加、下载、更新；负责终端运行状态监控 (POS 终端运行是否正常)，包括终端主动上报异常情况和终端管理平台下发监控命令两种方式。

[0069] POS 终端管理平台存储 POS 终端及商户信息，将这些信息提供给 POS 前置设备验证 POS 终端是否合法，商户是否合法。

[0070] 统一支付平台用于在线交易时，接收业务管理平台发来的用户信息及相关交易信息后，与银行系统进行实时交互完成银行账户的扣款；还用于离线交易时，接收业务管理平台发来的用户信息及相关交易信息后，采用日终方式完成。即统一支付平台是支持和具体商户结算、和资金系统相连的环节。统一支付平台与银行账务系统的接口，是银行账务系统接入移动支付系统的唯一入口，所有与银行关联的清算、对账信息都经由统一支付平台转

APPL-1002
APPLE INC. / Page 373 of 1892

发到业务管理平台进行处理。

[0071] 本实施例提供一种实现移动支付的方法，如图 2 所示，根据本发明实现移动支付的方法包括如下步骤：

[0072] 步骤 S2002，用户确认 POS 终端上显示的支付金额后，在 RF-SIM 的移动支付终端上选择“在线账户”进行支付，然后将移动支付终端靠近刷卡器，同时在 POS 附带的密码键盘上输入 PIN。

[0073] 步骤 S2004，MIS 商户装置获取移动支付终端的交易数据及用户的 PIN，并使用 PIK1 对 PIN 进行加密后连同交易数据及 POS 终端信息封装成标准 8583 联机交易报文（该报文包括应用类型标识 AID），并进行 MAC 生成，之后将报文发送至移动支付平台。

[0074] 该步骤中，可以是由位于 MIS 商户装置的 POS 终端生成上述 8583 联机交易报文，并进行 MAC 生成后发送至位于 MIS 商户装置的商户前置设备，商户前置设备收到上述报文后先进行 MAC 验证，验证通过后对该 8583 联机交易报文加封装企业代码后进行 MAC 生成，然后查询存储的 POS 终端与移动支付平台的对应关系后由数据专线将上述报文发送至对应的移动支付平台。

[0075] 步骤 S2006，移动支付平台收到 8583 联机交易报文后，先进行 MAC 验证，验证通过后对报文进行合法性检查，内容包括终端设备编号及运行状态、操作员、校验位以及 POS 终端的有效期等，用以判断交易请求的合法性以及是否做出拒绝。还需要校验 PIN 是否正确，若正确则完成本次账务处理后，返回交易响应。账务处理包括在线账户时修改在线账户信息等。

[0076] 该步骤具体包括：

[0077] a) 位于移动支付平台的 POS 前置设备收到 8583 联机交易报文后，先进行 MAC 验证，验证通过后对使用 PIK2 将 PIN 进行转加密（即重新用 PIK2 对 PIN 进行加密），重新封装一个移动支付平台内部通用的类 8583 报文后进行 MAC 生成，并根据报文中的 AID（应用类型标识），将交易报文转发至对应的应用平台进行处理；

[0078] b) 应用平台收到类 8583 报文后，先进行 MAC 验证，验证通过后对该类 8583 报文进行合法性检查，若合法则对类 8583 报文重新进行 MAC 生成后发送至业务管理平台；

[0079] c) 业务管理平台收到类 8583 报文先进行 MAC 验证，验证通过后校验 PIN 是否正确，之后完成本次交易的账务处理。

[0080] 在线交易时，统一支付平台接收业务管理平台发来的用户信息及相关交易信息后，与银行系统进行实时交互完成银行账户的扣款。

[0081] 对 PIN 进行校验可以是，将 PIN 密文、KEK（密钥加密密钥）加密下的 PIK2 以及本地存放的 PIN 密文等信息一并送入本地加密机，由加密机在其内部将业务管理平台上送的 PIN 和本地数据库中存放的 PIN 进行比较，完成 PIN 的校验。

[0082] 步骤 S2008，移动支付平台通过 MIS 商户装置向移动支付终端返回交易响应。

[0083] 在小额支付场景下，移动支付终端可以选择“现金账户”进行离线交易，此时无需使用 PIN。具体步骤如下：

[0084] 步骤 S3002，用户确认 POS 终端上显示的支付金额后，在 RF-SIM 的移动支付终端上选择“现金账户”进行支付，然后将移动支付终端靠近刷卡器；

[0085] 步骤 S3004，MIS 商户装置获取移动支付终端的交易数据以及移动支付终端的余

APPL-1002
APPLE INC. / Page 374 of 1892

额信息，验证本次交易是否合法，并验证该移动支付终端的现金账户余额是否足够本次交易，若交易合法且现金账户余额足够本次交易，则完成本次离线交易处理，包括扣除移动支付终端的现金账户余额。并采用日终清算方式交本次交易记录发送至移动支付平台。

[0086] 如图 3 所示，根据本发明的支付账户在线充值流程包括如下步骤：

[0087] 步骤 S4002，用户持现金及 RF-SIM 移动支付终端至营业厅 / 充值网点，POS 充值终端读取移动支付终端（卡）侧的用户信息后发送至柜面客户端。

[0088] 步骤 S4004，柜面客户端将用户信息发给业务管理平台，业务管理平台进行合法性验证，包括对用户卡、账户身份的验证；

[0089] 步骤 S4006，验证通过后由业务管理平台返回用户及其附属支付账户的详细信息，附属支付账户指在线账户和现金账户，这里返回的是两个账户在业务管理平台内存储的信息。

[0090] 步骤 S4008，柜面客户端根据用户要求选择充值账户（现金账户或在线账户），填写充值金额后将请求发给业务管理平台。

[0091] 步骤 S4010，业务管理平台根据请求进行账户合法性验证，修改现金账户 / 在线账户信息，生成充值记录。

[0092] 步骤 S4012，业务管理平台通过柜面客户端向移动支付终端返回充值结果信息。

[0093] 步骤 S4014，对于现金账户充值，还将由 POS 充值终端修改移动支付终端侧的现金账户信息。

[0094] 图 4 为根据本发明的密钥分配方式示意图。

[0095] 移动支付系统的密钥体系分为三层：主密钥 (MK)，用于对密钥加密密钥 KEK 进行加密保护，各加密机存储的 KEK 是经过 MK 加密的，MK 由本地加密机产生；

[0096] 密钥加密密钥 (KEK)，用于工作密钥在线更新时加密工作密钥；

[0097] 工作密钥 (WK)，包括对 PIN 加密的 PIK(PIN 加密工作密钥)，以及进行报文鉴别 (MAC) 的 MAK(MAC 加密工作密钥)。

[0098] MAK 是由 POS 前置设备产生，各区域（即网元）的 MAK 一致，但由不同的 KEK 进行加密。

[0099] 密钥分配的目的首先是使主机之间分别共享相同的传输密钥 (KEK)，以便工作密钥的安全传输。然后便可定时生成工作密钥进行加密下传，从而保证通讯的双方具有相同的工作密钥。下面将对移动支付系统中的密钥分配方式进行简要说明（图 4，以 PIK 为例）

[0100] 1)POS 终端的工作密钥 PIK1 由 POS 前置设备产生，POS 前置设备中用于 PIN 转加密的 PIK2 由业务管理平台产生。PIK 在不同区域（即网元）中由不同的 KEK 保护，这些 KEK 由本地加密机产生，通过 IC 卡等方式注入下一通信网元的加密机中，即将本地产生的 KEK 存储到与之相连的下一级通信网元。

[0101] 2) 密钥分段有效原则：每个 KEK 仅在某一区域（即网元）内存在并有效，不同区域（即网元）间的 KEK 之间没有任何关系。用以保证不会因某个区域（即网元）的 KEK 的泄露而影响其它区域间传输的数据的安全，从而实现密钥的分工管理。

[0102] 本发明提出了一种基于 RF-SIM 和 ISO8583 协议的安全移动支付方法，用于快速、有效、安全地对非接触式移动支付交易进行处理。

APPL-1002
APPLE INC. / Page 375 of 1892

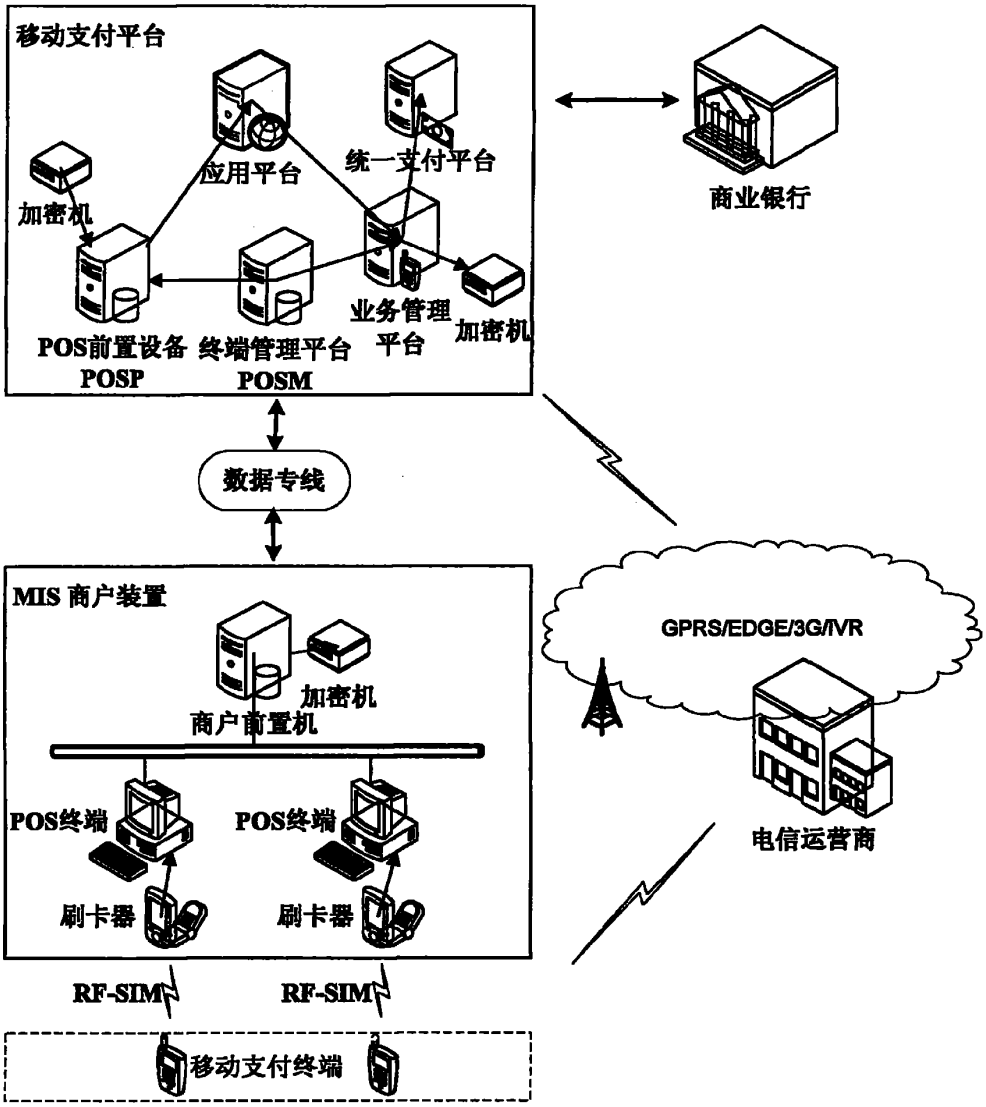


图 1

APPL-1002
APPLE INC. / Page 376 of 1892

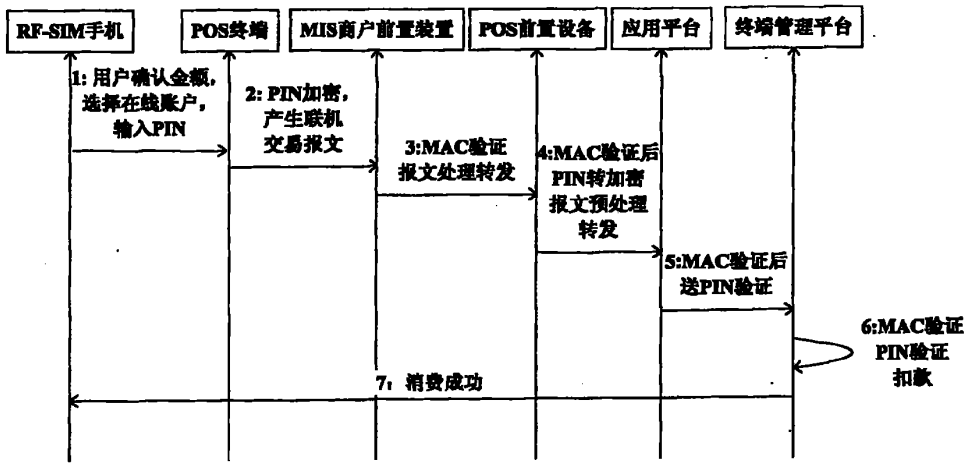


图 2

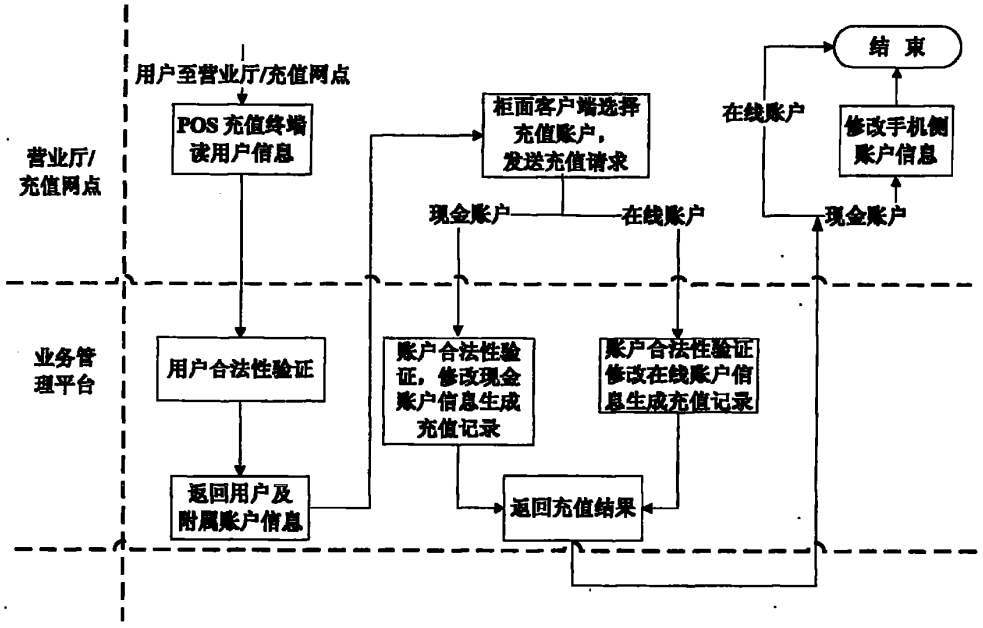


图 3

APPL-1002
APPLE INC. / Page 377 of 1892

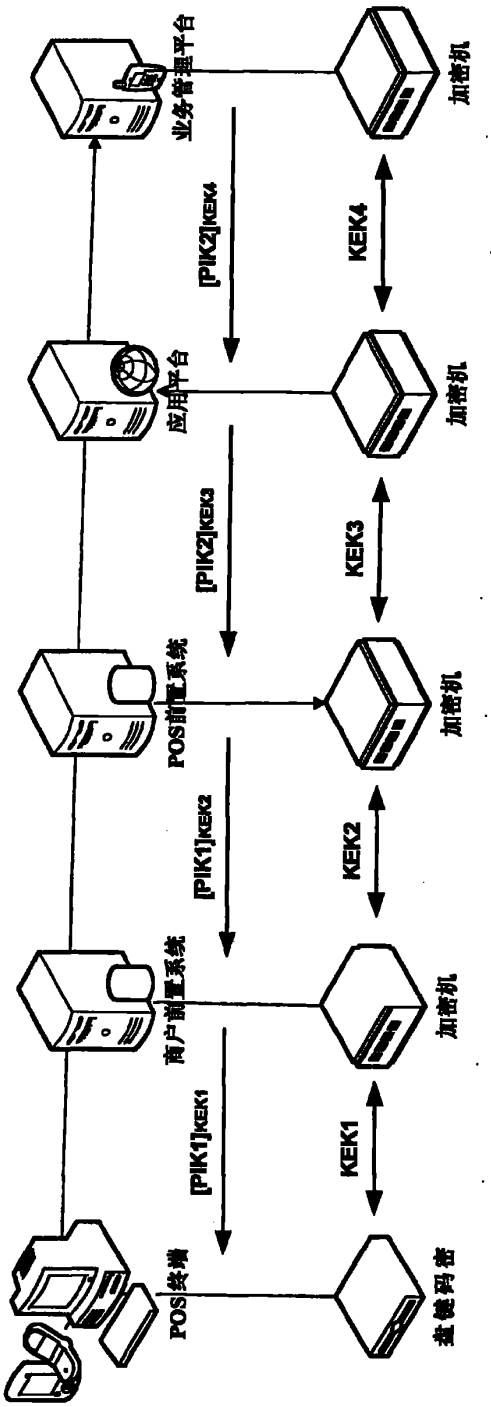


图 4

APPL-1002
APPLE INC. / Page 378 of 1892

Espacenet
Patent search
Deutsch English Français
Contact
Change country
About Espacenet Other EPO online services
Search My patents list (0) Data base Settings Help

DE10119808 (A1)
Bibliographic data
Description
Claims
Mosaics
Original document
Cited documents
Citing documents
INPADOC legal status
INPADOC patent family

Quick help
- What does A1, A2, A3 and B stand for after a publication number?
- What happens if I click on "In my patents list"?
- What happens if I click on the "Register" button?
- Why are some sidebar options deactivated for certain documents?
- How can I bookmark this page?
- Why does a list of documents with the heading "Also published as" sometimes appear, and what are these documents?
- What is a cited document?
- What are citing documents?
- What information will I find if I click on the link "View all"?
- Why do I sometimes find the abstract of a corresponding document?
- What happens if I click on the button "Translate this text?"

Bibliographic data: DE10119808 (A1) — 2002-09-12

In my patents list EP Register Report data error Print

Transaction method for providing goods or services involves vending machine comparing transaction codes transmitted to it and to customer from terminal at chargeable connection

Page bookmark DE10119808 (A1) - Transaction method for providing goods or services involves vending machine comparing transaction codes transmitted to it and to customer from terminal at chargeable connection

Inventor(s): HOLLAND CHRIS [DE] +

Applicant(s): HOLLAND CHRIS [DE] +

Classification: - **international:** *G06Q20/00; G07F5/18;* (IPC1-7): G06F17/60

- **European:** G06Q20/04; G06Q20/32; G07F5/18

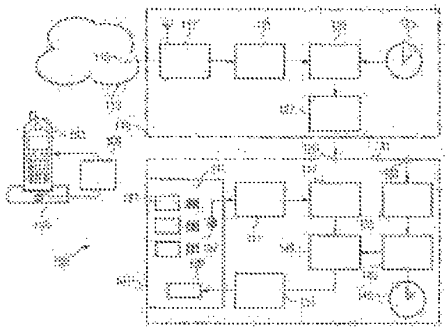
Application number: DE20011019808 20010423

Priority number(s): DE20011019808 20010423; DE20011009821 20010301

Abstract of DE10119808 (A1)

Translate this text into i
German Translate Powered by EPO and Google

The method involves making a connection between a calling customer terminal or payment point and a called terminal or payment point at a chargeable connection, sending object and vending machine identification data to the called terminal, generating a transaction code and sending to the customer terminal and vending machine, storing a reference code in the vending machine, entering the code to the vending machine, comparing codes and dispensing. The method involves making a connection between a calling customer terminal or payment point and a called terminal or payment point at a chargeable connection, sending goods or service object identification data and vending machine identification data to the called terminal, generating a transaction code and sending to the customer terminal and to the vending machine, storing the transmitted or generated transaction code as a reference code in the vending machine, the customer entering the code to the vending machine, comparing codes and dispensing the goods or service. Independent claims are also included for (1) a transaction method for providing functionality (2) an arrangement for providing goods or services; and (3) an arrangement for providing functionality. ,



Sitemap Accessibility Legal notice Terms of use Last updated: 28.02.2012 Worldwide Database 5.7.36; 93p

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 280 115 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.01.2003 Bulletin 2003/05

(51) Int Cl.[7]: **G07F 19/00**, G07F 7/08

(21) Application number: **02015629.5**

(22) Date of filing: **16.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.07.2001 JP 2001222163**
29.01.2002 JP 2002020410

(71) Applicant: **NTT DoCoMo, Inc.**
Tokyo 100-6150 (JP)

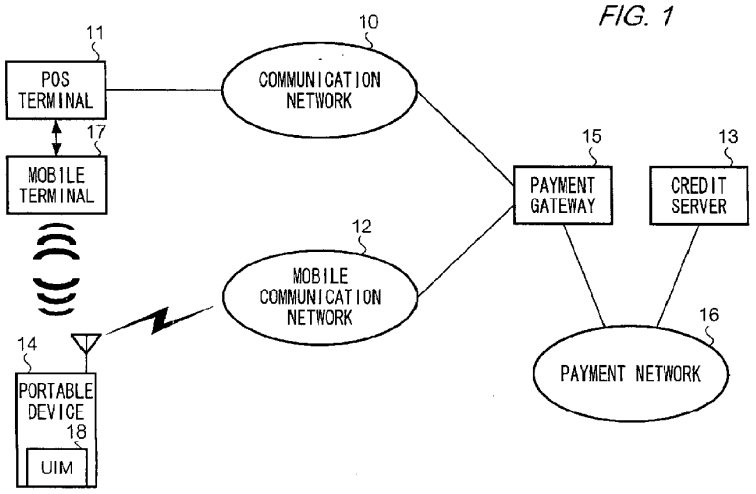
(72) Inventors:
- **Kinoshita, Masaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yoshida, Junichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakajima, Atsushi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tanaka, Manabu, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Hanada, Kazutoyo, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Yasuda, Jun, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Tomita, Syuichi, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Nakamura, Taijiro, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**
- **Ishibashi, Hideaki, NTT DoCoMo, Inc., Chiyoda-ku, Tokyo 100-6150 (JP)**

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Electronic payment method, system, and devices

(57) A portable device authenticates a user of the portable device. If authenticity of the user is confirmed, a user ID is transmitted to a POS terminal. Upon receipt of the user ID, the POS terminal sends a request for payment including the user ID and transaction information to a payment gateway. Upon receipt of the request, the payment gateway sends an e-mail to the portable device to execute an application for payment stored in the portable device.

FIG. 1



EP 1 280 115 A2

Printed by Jouve, 75001 PARIS (FR)

Description

Background of the Invention

Field of the Invention

[0001] The present invention relates generally to a method, system, and devices used for electronic financial transactions between financial institutions connected by a network.

Description of the Related Art

[0002] Electronic payment using a credit card is known in the art. As an example, a prior system for electronic payment is shown in fig. 21.

[0003] When a people (purchaser) buys goods at a shop, firstly, a clerk inputs transaction data including the name of goods, quantity, price, and tax into a Point of Sales (POS) terminal 1 provided at the shop. Secondly, he/she hand his/her credit card to the clerk. Thirdly, the clerk sets the card to a Card reader 2. Card reader reads out information such as a card number and expiration date stored in the card. Next, this card information is supplied to POS terminal 1. Upon receipt the information, POS terminal 1 makes a request for credit by adding information on the shop (merchant) to the card information and transaction data and sends it to a Credit server 4 managed by a credit card company via a Network 3 such as Credit Finance Information Switching Systems (CAFIS). Credit server 4 checks the card information included in the request sent by POS terminal 11. Finally, if Credit server 4 accepts authenticity of the card, it sends a completion message to POS terminal 1. In such a system, a consumer buys goods without carrying cash.

[0004] However, it is known that there is a security concern in such a system. Since a purchaser has to hand his/her credit card to a clerk in paying by a credit card, there is a danger that unauthorized persons improperly use the card. Furthermore, there is always a possibility of dropping off a credit card. In other words, a consumer necessarily takes risks that a stranger uses his/her credit card illegally.

[0005] The present invention has been made with a view to overcome the above problem and it is an object of the present invention to provide a method, system, server, terminal, computer program, and storage medium to conduct electronic financial transactions.

Summary of the Invention

[0006] To achieve the above aim, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

storing an authentication result of the user, by the user terminal when the user terminal confirms authenticity of the user;

transmitting a user identification information stored beforehand in the user terminal to a merchant terminal when the user terminal confirms authenticity of the user, by the user terminal;

transmitting to payment device via a first communication network the user identification information and transaction information transmitted from the user terminal, by the merchant terminal;

receiving the user identification information and the transaction information transmitted from the merchant terminal, by the payment device;

identifying the user terminal on the basis of the user identification information and transmitting commands for instructing transmission of the authentication result to the user terminal via a second communication network;

transmitting authenticity of the user to the payment device via the second communication network if the user terminal stores authenticity of the user, by the user terminal; and

performing payment processing on the basis of the transaction information upon receipt of the authenticity from the user terminal, by the payment device.

[0007] In an electronic payment system in which the above method is applied, a user is able to pay by credit card using a terminal without handing a credit card to a clerk, thereby preventing a third-party including a clerk from using the card improperly. Furthermore, since the user terminal authenticates a user, if a third-party obtains a user terminal improperly, the terminal cannot be used for payment in the electronic payment system by the third-party. Furthermore, the payment device identifies a user to which authentication result is transmitted. In other words, the only user terminal that the payment device specifies can proceed payment processes. Thus, the danger of an improper use by a third-party of the user terminal is reduced. Furthermore, the user terminal transmits an authentication result according to the commands send from the payment device, in other words, a user does not have to operate the user terminal for the transmission. Therefore, the danger of stop of payment processing due to misoperation by a user is prevented.

[0008] In a preferred embodiment, an electronic payment method of the present invention comprises the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to the user terminal by the user, by the user terminal;

transmitting user identification information for identifying a user to a merchant terminal, by the user terminal, when the user terminal confirms authen-

APPL-1002
APPLE INC. / Page 381 of 1892

ticity of the user;
transmitting to a payment device via a first commutation network the user identification information transmitted from the user terminal, by the merchant terminal;
receiving the user identification information from the merchant terminal, by the payment device;
identifying the user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in the user terminal to identified user terminal via a second communication network, by the payment device;
upon receipt of the commands, executing the application to transmit a request for proceeding payment processing to the payment device via the second communication network, by the user; and
upon receipt of the request from the user terminal, performing a payment processing.

[0009] In this embodiment the payment device identifies a user terminal on the basis of user identification information and sends commands so that the user terminal can execute application for payment stored in the user terminal. In other words, both a user and a user terminal are authenticated, thereby ensuring security against authorized person greatly. In addition, a user's convenience is improved because a user does not have to carry out troublesome operation necessary for payment.

[0010] In another embodiment, an electronic payment method comprises the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit;
retrieving from a storage unit a card number corresponding to the
identified user, by a retrieving unit;
encrypting the retrieved card number, by an encrypting unit;
generating a key for decryption of the encrypted card number, by a generating unit;
transmitting to the merchant terminal the encrypted card number, by a first transmitting unit; and
transmitting the key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

[0011] In an electronic payment system in which a method of this embodiment of the present invention is used, a user is able to pay by credit card to a merchant in a way that the merchant does not know a card number because a credit card number is encrypted for transmission to the merchant. Specifically, a payment device determines a card to be encrypted on the basis of the user identification information. On the other hand, the credit server obtains a card number by decrypting an encrypted card number using the key for decryption received from the payment device, thus the credit server is able to carry out payment processing. Further, since the encrypted card number is generated each time a transaction is conducted, the merchant can manage sales at the shop using the encrypted card number although the merchant does not know card numbers.

[0012] An electronic payment system of the present invention has a payment device, a merchant terminal connected with the payment device via a first communication network, and a user terminal connected with the payment device via a second communication network and is characterized in that:

the user terminal authenticates a user of the user terminal on the basis of user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, stores authentication result; and
transmits to the merchant terminal user identification information stored in the user terminal;
the merchant terminal transmits to the payment device via the first communication network the user identification information transmitted from the user terminal and transaction information;
the payment device identifies the user terminal on the basis of the user identification information transmitted from the merchant terminal and
transmits to the identified user terminal via the second communication network commands for instructing transmission of the authentication result;
the user terminal transmits to the payment device via the second communication network according to the commands transmitted from the payment device when the user terminal stores the authentication result; and
upon receipt of the authentication result from the user terminal, the payment device performs payment processing on the basis of the transaction information.

[0013] In a preferred embodiment, an electronic payment system of the present invention is characterized in that:

the user terminal authenticates a user on the basis of the user identification information inputted to the user terminal by the user;
if authenticity of the user is confirmed, transmits to the merchant terminal a user identification information for identifying the user;
the merchant terminal transfers the user identification information to the payment device via the first communication network;
the payment device identifies the user terminal on the basis of the user identification information and transmits to the identified user terminal via the second communication network commands for execut-

APPL-1002
APPLE INC. / Page 382 of 1892

ing an application for payment stored in the user terminal;
the user terminal executes the application according to the commands and
transmits a request for proceeding payment processing to the payment device via the second communication network; and
the payment device performs the payment processing according to the request.

[0014] A communication terminal used for an electronic payment system of the present invention has a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network and comprises:

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a storing means for storing an authentication result when authenticity of the user is confirmed by the authenticating means;
a storage medium for storing the user identification information;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
a receiving means for receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network; and
a second transmitting means for transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0015] In a preferred embodiment, a communication terminal used for the electronic payment system comprises:

an authenticating means for authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
a first transmitting means for transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from the payment device via the second communication network; and
a second transmitting means for executing the application for payment stored in the user terminal and transmitting, according to the application, a request for proceeding payment processing to the payment device via the second communication network.

[0016] A payment device of the present invention comprises:

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying the user terminal among registered user terminal on the basis of the received user identification information; a transmitter for transmitting to the identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via the second communication network after transmission of the commands.

[0017] In another embodiment, a payment device comprises:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information;
a retrieving unit for retrieving from the storage unit a card number corresponding to the identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of the encrypted card number;
a first transmitting unit for transmitting to the merchant terminal the encrypted card number; and
a second transmitting unit for transmitting the key to a credit server managed by an issuer of the credit card.

[0018] A computer program product of the present invention makes a computer incorporated into a communication terminal used for the electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with the payment device via a first communication network to execute the steps of:

APPL-1002
APPLE INC. / Page 383 of 1892

authenticating a user of the communication terminal on the basis of a user identification information inputted to the user terminal by the user;
storing an authentication result into a storage means when authenticity of the user is confirmed by the authenticating means;
transmitting, when authenticity of the user is confirmed, the user identification information stored in the storage means to the merchant terminal so that the merchant terminal transmits to the payment device a request for payment processing including the user identification information;
receiving commands for instructing transmission of the authentication result which is transmitted, in response to the request for payment, from the payment device via the second communication network; and
transmitting, upon receipt of the commands, a request for proceeding the payment processing including the authentication result to the payment device via the second communication network.

[0019] In another embodiment, a computer program product makes a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to the identified user;
encrypting the retrieved card number;
generating a key for decryption of the encrypted card number; transmitting to the merchant terminal the encrypted card number; and
transmitting the key to a credit server managed by an issuer of the credit card.

[0020] A storage medium of the present invention stores the above computer program products.

Brief description of the drawings

[0021]

Fig.1 is a conceptual block diagram to illustrate an electronic payment system based on the first embodiment of the present invention.
Fig.2 is a block diagram to illustrate a portable device used in the system.
Fig.3 illustrates a UIM mounted detachably to the portable device.
Fig.4 shows a storage area of EEPROM in the UIM.
Fig.5 is a block diagram to illustrate a POS terminal and a mobile terminal used in the system.
Fig.6 is a block diagram illustrating a payment gateway used in the system.
Fig.7 illustrates data items stored in a user table in a hard drive of the gateway.
Fig.8 illustrates data items stored in a transaction table in a hard drive of the gateway.
Fig.9 illustrates data items stored in an issuer table in a hard drive of the gateway.
Fig.10 illustrates data items stored in a merchant table in a hard drive of the gateway.
Fig.11 is a sequence flowchart illustrating payment processing in the system.
Fig.12 is a flowchart illustrating a processing performed by the portable device.
Fig.13 illustrates a screen displayed on a display of the portable device.
Fig.14 is a flowchart illustrating a processing performed by the portable device.
Fig.15 is a flowchart illustrating a processing performed by the portable device.
Fig.16 illustrates a screen displayed on a display of the portable device.
Fig.17 illustrates a screen displayed on a display of the portable device.
Fig.18 is a flowchart illustrating a processing performed by the POS terminal.
Fig.19 is a flowchart illustrating a processing performed by the payment gateway.
Fig.20 is a conceptual block diagram illustrating an electronic payment system based on a modification of the first embodiment.
Fig.21 illustrates an electronic payment system of the prior art.
Fig.22 illustrates an electronic payment system based on the second embodiment.
Fig.23 illustrates an example of date items stored in a POS terminal.
Fig.24 illustrates an example of date items stored in a credit server.
Fig.25 illustrates an example of date items stored in a storage unit of a payment gateway.
Fig.26 is a flowchart illustrating a method for payment used in the system.
Fig.27 is a flowchart illustrating a method for payment used in the system.
Fig.28 is a conceptual block diagram to illustrate a computer program for payment based on the second embodiment.

Detailed Description

(First embodiment)

[0022] The first embodiment of the present invention will now be described referring to the drawings.

A. Configuration of the system

A-1. Overall configuration

[0023] Fig. 1 shows that a system to which a method for electronic payment of the present invention based

APPL-1002
APPLE INC. / Page 384 of 1892

on the first embodiment is applied. As shown therein, the system comprises (a) a POS terminal 11 connected to a communication network 10, (b) a payment gateway 15 connected to Communication network 10, a mobile communication network 12, and a payment network 16, (c) a portable device 14 by which a user obtains communication services via Mobile communication network 12, (d) a credit server 13 connected to Payment network 16, and (e) a mobile terminal 17. For the sake of simplicity, only one POS terminal 11 and one Portable device 14 is shown in the figure. In actuality, a plurality of POS terminals are connected to Communication network 10 and many portable devices are connected to Mobile communication network 12.

[0024] A mobile communication network 12 includes mobile telephone networks in which Personal digital Cellular (PDC) scheme, Code Division Multiple Access (CDMA) scheme, or other schemes is used and data communication networks in which PDC-Packet (PDC-P) scheme is used. Each network has base stations which are not shown. Each base station covers an area and carries out radio communications with portable devices 14 within the area. Therefore, Portable device 14 is able to carry out voice and data communications by radio via Mobile communication network 12. A payment gateway 15 is connected to Mobile communication system 12, thus Portable device 14 is able to carry out data communications with Payment gateway 15.

[0025] A POS terminal 11 and Payment gateway 15 are connected via Communication network 10. Specifically, Communication network 10 is a dedicated line to which many POS terminals 11 and Gateway system 15 are connected. Needless to say, Communication network 10 can be a fixed telephone network, a public network such as Internet, or a mobile communication network (possibly Mobile communication network 12).

[0026] A credit server 13 managed by a credit company and Gateway system 15 are connected via a payment network 16. Specifically, Payment network 16 is designed especially for credit payment such as Credit and Finance Information Switching Systems (CAFIS). Credit server 13 is a conventional server for credit payment. Specifically, upon receipt of a request for credit transmitted by a POS terminal via Payment network 16, Credit server 13 checks authenticity of a credit card. If the authenticity is confirmed, Server 13 carries out a payment processing before sending a completion message to the POS terminal.

[0027] An essence of the electronic transaction service using a method for paying electronic transactions based on this embodiment is as follows. When a user of Portable device 14 buys goods at a shop, the user uses Portable device 14 to make request for payment to Credit server 13 via POS terminal 11 and Payment gateway 15. As such, a user is able to pay without handing a credit card to others including a clerk. Components of this system will be described in detail below.

A-2. Portable device

[0028] Portable device 14 has a function of carrying out wireless voice and data communications via Mobile communication network 12. Further, it has a function of carrying out short-range radio communication using Bluetooth, for example, to carry out data communications with POS terminal. In addition, the device 14 is able to mount a User Identity Module (UIM) detachably.

[0029] As shown in fig.2, Portable device 14 has a control unit 310, memory 320, control unit 330, communication unit 340, mic/speaker 350, UIM interface 360, and radio interface 370.

[0030] Control unit 310 has a Central processing unit (CPU) and other microprocessors to execute programs stored in Memory 320 to control each unit of the device 14 including reading/writing data from/to UIM 18.

[0031] Memory 320 includes a Read Only Memory (ROM), a Random Access Memory (RAM), and an Electrically Erasable and Programmable ROM (EEPROM) and has several storage areas, one of which is assigned for storing programs including programs for starting and proceeding payment described later, and another one of which is for storing data. Another program stored in Memory 320 is used for browsing, in other words, accessing a Web server on the Internet, downloading Hyper Text Markup Language (HTML) data or Compact-HTML (C-HTML) data, and displaying the data. Another one is used for sending and receiving e-mail. Control unit 310 executes these programs so that the user can browse and use e-mail.

[0032] Input device 330 has operation buttons such as a ten-key pad, which is not shown in the figure, to input information such as a telephone number and to select buttons or icons displayed on a liquid crystal display not shown in the figure. Communication unit 340 transmits data such as information on ordering via an antenna 341 under control of Control unit 34 land receives data send via Antenna 341. Mic/speaker 350 includes a microphone to input a sound and a speaker to output a sound.

[0033] UIM interface 360 supplies information outputted from Control unit 310 to UIM 18 and information outputted from UIM 18 to Control unit 310. Information stored in UIM 18 is used each time a user carries out voice and data communications by radio via Communication network 12. Radio interface 370 is used to carry out short-rage communication with POS terminal 11 by Bluetooth, for example.

A-3. UIM

[0034] As shown in fig.3, UIM 18 is an Integrated Circuit (IC) card which is detachable/attachable and includes a CPU 210, interface 215, ROM 220, RAM225, and EEPROM 230. UIM 18 stores information unique to the user including a subscriber number and telephone book used for carrying out communication via Mobile

APPL-1002
APPLE INC. / Page 385 of 1892

communication network 12.

[0035] CPU210 executes a control program stored in ROM 220 to control each unit within UIM 18. Interface 215 connects UIM 18 with Portable device 14. ROM 220 is a nonvolatile memory and stores programs for analyzing and executing commands supplied from Portable device 14 and for managing data, for example, as well as the control program. RAM 225 is a rewritable memory for temporarily storing data supplied from Portable device 14. EEPROM 230 is a versatile and is rewritable. EEPROM 230 stores information necessary for communication with Portable device 14.

[0036] Fig.4 shows storage areas in EEPROM. As shown, EEPROM 230 has storage areas 231 and 233.

[0037] Storage area 231 stores subscriber numbers, outgoing history, incoming history, talk time, telephone book data, and other information specific to user(s) of UIM 18. Storage area 233 stores information used when Portable device 14 starts a payment operation. Specifically, a device ID for identifying Portable device 14 uniquely is stored. For example, a user registers, in advance, Portable device 14 at a provider of this electronic financial transaction service to obtain the service using the device 14. After the registration, the provider gives the user the device ID.

[0038] In addition, Storage area 233 stores an address such as Uniform Resource Locator (URL), to connect with Payment gateway 15. Further, Storage area 233 stores pairs of a user ID and a password, each of which is used for an application for payment executed at the Portable device 14 when the user uses the electronic payment service. If the user possesses two or more credit cards, it is possible that each pair of a user ID and a password corresponds to each credit card. Furthermore, Storage area 233 has an area for authentication results which is used for the payment application.

[0039] When UIM 18 is attached to Portable device 14, information stored in UIM 18 can be supplied to Portable device via UIM interface 360, thereby allowing for Portable device 14 to carry out various functions including radio communication.

A-4. POS terminal

[0040] POS terminal 11 is installed at a shop of a merchant participating in the electronic payment service. POS terminal 11 stores data necessary for managing information on financial transactions, sales, and customers, for example.

[0041] As shown in fig.5, POS terminal 11 has a control unit 710, a display 720, communication interface 730, and an interface 740.

[0042] Control unit 710 includes a CPU, a ROM, and a RAM and controls all units of POS terminal 11. Control unit 710 has the same function as a general POS terminal for managing information on financial transactions, sales, and customers. In addition, Control unit 710 has functions of controlling each unit to perform processing necessary for the electronic payment service. Display 720 includes a liquid crystal panel, for example, on which information on merchandise such as a name, price, quantity, tax, and total amount is displayed. Communication interface 730 carries out communication with Gateway system 15 via Communication network 10. Interface 740 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication.

[0043] Mobile terminal 17 is, for example, a Personal Digital Assistants (PDA) or a laptop computer, which includes a control unit 810, interface 820, display 840, and radio interface 830.

[0044] Control unit 810 includes a CPU, ROM, RAM, and other modules and controls all units of POS terminal. Control unit 810 has the same functions as a general mobile terminal such as PDA. In addition, Control unit 810 has a function of controlling each unit to carry out processing necessary for the electronic transaction service.

[0045] Display 840 includes a liquid crystal panel to display information, for example. Interface 820 is, for example, a general interface such as RS-232C or Universal Serial Bus (USB). POS terminal 11 is connected to Mobile terminal 17 through a cable to carry out data communication. Radio interface 830 features short-range wireless communication with Portable device 14 via Bluetooth, for example.

A-5. Payment gateway

[0046] Payment gateway 15 for providing the electronic payment service using a method for electronic payment based on this embodiment is installed by a provider of the service. As shown in fig.6, Payment gateway 15 includes a payment server 150 connected to a Local Area Network (LAN), direction server 160, and a network interface (I/F) 170.

[0047] Network interface 170 is, for example, a router. Payment server 150 and direction server 160 exchanges data with POS terminal 10, Portable device 14, and Credit server 13 via Communication network, Mobile communication network, and Payment network 16, respectively.

[0048] Payment server 150 may be a personal computer or a workstation, including a CPU 151, ROM 152, RAM 153, hard drive 154, and LAN interface 155. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD), allowing an administrator of Gateway system 15 to make reconfigurations including registration of users.

[0049] LAN interface 155 is used for exchange of data between Network interface 170 and Direction server 160 connected to the LAN.

[0050] CPU 151 performs arrhythmic computation as well controls each unit of Payment server 150. ROM 152

APPL-1002
APPLE INC. / Page 386 of 1892

stores programs to be read out and executed by CPU 151. CPU uses RAM 153 as a work area.

[0051] Hard drive 154 stores application programs and data to be read out and executed by CPU 151 to control each unit for provision of the electronic transaction service. Hard drive 154 includes a user table 154a, transaction table 154b, issuer table 154c, and merchant table 154d.

[0052] As shown in fig.7, user table 154a has four areas for user ID 154aa, password 154ab, terminal ID 154ac, and credit card number 154ad. A staffer of the provider of this service inputs the above information into User table 154a when a user subscribes to the service. It is possible that, if a subscriber has more than two credit cards and wants to obtain the service using these credit cards, the subscriber (user) has a plurality of user IDs each of which is corresponding to each credit card.

[0053] Area 154aa stores user IDs each of which identifies a subscriber uniquely. Area 154ab stores passwords each of which is used for authentication of a user. Area 154ac stores identification information each to identify Portable device 14 used for the electronic transaction service. The user IDs, passwords, and identification information stored in Hard drive 154 are the same stored in Storage area 233 in EEPROM 230 of UIM18 shown in fig. 4 Area 154ad stores credit card numbers of users. If a user has two or more credit cards, the user can specify one or more credit cards to be used for this service and thus stored in Area 154ad when the user subscribes to the service. In addition, Area 154ad stores expiration dates of the cards, which are not shown in the figures.

[0054] Referring back to fig. 6, Transaction table 154ab has areas for storing details of transactions conducted by users. Specifically, as shown in fig. 8, Transaction table 154ab corresponding to a subscriber having a user ID "00001" has four areas for transaction 154ba, for date 154bb, for merchant number 154bc, and for transaction details 154bd. Area 154ba stores IDs each of which identifies a transaction conducted by a user. It is noted that CPU 151 gives a transaction ID every time a transaction is conducted. Area 154bb stores dates and times of transactions each corresponding to each transaction ID. Area 154bc stores merchant numbers each identifying a shop where the transaction was conducted. A unique merchant number is assigned to all merchants in advance. Area 154bd stores details of transactions each corresponding to each transaction ID. Specifically, merchandise name, quantity, price, tax, payment method (lump-sum, installment, payment with bonus, payment partially with bonus, and, revolving, for example), and other related information on the transaction.

[0055] Referring again to fig. 6, Issuer table 154c stores information on credit companies and credit cards available for the service. Specifically, as shown in fig. 9, Issuer table 154c has three areas. Area 154ca stores ranges of card numbers. Area 154cb stores company codes each of which identifies corresponding credit company. Area 154cc stores names of credit companies. For example, fig. 9 shows that a credit card whose number lies within a range between "1525000000" and "1525059999" is issued by credit company "A".

[0056] Referring again to fig. 6, Merchant table 154d stores information on which cards and which methods of payment are available at a shop. Specifically, as shown in fig. 10, Merchant table 154d has four areas of 154da, 154db, 154dc, and 154dd. Area 154da stores codes each of which identifies each merchant. Area 154db stores merchant's names. Area 154dc stores codes each of which identifies a credit company, namely, issuer of a credit card available for the merchant, which is the same stored in Area 154cb shown in fig. 9. Area 154dd stores credit company's names. Area 154de stores payment methods in which a user can pay by a card. As an example, fig.10 shows that a user is able to arrange payment in a lump-sum, installments, or revolving system but neither payment with bonus nor payment partially with bonus is accepted. "L", "I", "B", "pB", and "R" represents lump sum, installments, bonus, bonus (partially), and revolving, respectively. Furthermore, detailed information such as the number of payment in installments and an available period in payment with bonus may be stored.

[0057] Direction server 160 will now be described referring to fig. 6. Direction server 160 may be a personal computer or a workstation, including a CPU 161, ROM 162, RAM 163, hard drive 164, and LAN interface 165. Further, Payment server 150 includes an input device such as a keyboard and Cathode-ray Tube (CRT) or Liquid Crystal Display (LCD). Detailed description of these devices is omitted.

[0058] LAN interface 165 is used for exchange of data between Network interface 170 and Payment server 150 connected to the LAN. CPU 161 performs arrhythmic computation as well controls each unit of Direction server 160. ROM 152 stores programs to be read out and executed by CPU 161. CPU uses RAM 163 as a work area. Hard drive 164 stores application programs and data to be read out and executed by CPU 161, to control each unit for provision of the electronic payment service. In addition, Hard drive 164 stores a mail box 164a used for the electronic transaction service. To be more specific, Mail box 164a includes mailboxes each corresponding to an e-mail account of Portable device 14.

[0059] Upon receipt of a request from Payment server 150, CPU 161 generates and stores e-mail into a mail box assigned to each Portable device 14 in Mail box 164a and sends a reception message to the Portable terminal 14 having an address indicated by the request. Upon receipt of the reception message, Portable device 14 accesses Mailbox 164a via Mobile communication network to obtain e-mails for Portable device 14. Namely, Direction server 160 a function as a mail server with features including sending a reception message.

APPL-1002
APPLE INC. / Page 387 of 1892

B. Operations of the system

B-1. Overall sequence of the operations

[0060] An outline of sequence of operations carried out in this electronic payment system will now be described.

[0061] Fig. 11 is a sequence flowchart showing an outline of sequence of operations in which a user of Portable device 14 conducts a transaction (purchases goods) at a shop at which POS terminal 11 and Mobile terminal 17 are installed and obtains this electronic payment service for payment using Portable device 14.

[0062] As shown in fig. 11, firstly, a clerk inputs information on a transaction including a merchandise name, quantity, price, tax into POS terminal 11 at a shop. If a purchaser wants to pay using this electronic payment service, the purchaser operates his/her Portable device 14 to execute an application program for the electronic payment. And an input screen for a user ID and a password to be used for authentication is displayed on a display of Portable device 14.

[0063] The purchaser (the user of Portable device 14) operates ten-key pad or the like, to input a user ID and a password. Portable device 14 checks the user ID and password against those stored in UIM 18, to authenticate the user (step S1).

[0064] If the authentication failed, Portable device 14 notifies the user that the user is not a right person and thus rejected before carrying out error processing, for example, terminating the processing. If the authentication is completed, Portable device 14 sends the user ID stored in UIM 18 to Mobile terminal 17 by short-range wireless communication. The user ID is transferred from Mobile terminal 17 to POS terminal 11 (step S2). In addition, Portable device 14 stores the authentication result representing authenticity of the user into Storage area 233 of UIM18. It is noted that Mobile terminal 17 is omitted in fig. 1, for sake of simplicity. But in reality data is exchanged via Mobile terminal 17 between POS terminal 11 and Portable device 14.

[0065] Upon receipt of a user ID sent from portable device 14 via Mobile terminal 17, POS terminal 11 sends to Payment gateway 15 via Communication network 10 transaction information, the user ID, and a request for transaction number including information to identify the shop (merchant), which is inputted buy a clerk (step S3). Upon receipt of the request sent from POS terminal, Payment gateway 15 stores the transaction information included in the request into Transaction table 154b and adds a transaction number to the transaction information to send back to POS terminal 11 via Communication network 10 (step S4).

[0066] Further, Payment gateway 15 sends an e-mail including commands for direction of payment to Portable device 14 indicated by the user ID included in the request (step S5). Upon receipt of the e-mail sent from Payment gateway 15 via Mobile communication system 12, Portable device 14 executes an application for payment according to the commands included in the e-mail.

[0067] Specifically, the authentication result and the device ID both stored in UIM 18 are transmitted to Payment gateway 15 via Mobile communication network 12, to make a request for proceeding payment processing (step S6). Therefore, the user need not do complicated procedures for payment, for example inputting information on the transaction which is often bothersome for a user. In this system a request for proceeding payment processing is sent to Payment gateway 15 automatically after completion of the authenticity.

[0068] Upon receipt of the authentication result and the request including the device ID both sent from Portable device 14 via Mobile communication network 12, Payment gateway 15 confirms authenticity of the user through the result. Next, Payment gateway 15 authenticates the Portable device 14 by checking the device ID (step S7). Specifically, Payment gateway 15 checks the device ID sent from Portable device 14 against a device ID stored correspondingly to the user ID in User table 154a. If the two IDs coincide, authenticity of Portable device 14 is established. Otherwise Payment Gateway 15 stops payment processing.

[0069] If the authenticity of Portable device 14 is established, Payment gateway 15 sends to Portable device 14 via Mobile communication network 12 transaction details including name of goods, quantity, and price and information on possible payment methods (step S8). Upon receipt of a payment method and a confirmation from Portable device 14 (step S9), Payment gateway 15 retrieves transaction information from Transaction table 154b and a credit card number and its expiration date from User table 154a. Next, Payment gateway 15 sends to Credit server 13 via Payment network 16 a request for credit including information on the merchant and the payment method along with the retrieved transaction information (step S10).

[0070] Upon receipt of the request, Credit server 13checks the credit card number and its expiration date, to determine whether to conduct the payment processing. If the credit card number and the expiration date are proper, Credit server 13 carries out payment processing (step S11) and sends a completion report to Payment gateway 15 via Payment network 15 (step S12). This report is transferred from Payment gateway 15 to POS terminal 11 via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step S13 and step S14, respectively). B-2. Operations of portable device

[0071] It will now be described that processing carried out by Portable device 14 when a user obtains the electronic payment service. As shown in fig. 12, if a user wants to use the service using his/her Portable device 14 when purchasing goods at a shop, the user inputs with Input device 330 a direction for Portable device to execute an application for payment. Control unit 310 of Portable device 14 displays credit cards available for the

APPL-1002
APPLE INC. / Page 388 of 1892

user on a display.

[0072] An example of a screen for selection of a credit card displayed on a display of Portable device 14 is shown in fig.13. This screen shows a list of credit cards registered in advance by the user at a provider of the service. When the user operates Input device 330 to select a check box and clicks an "OK" button, a credit card for use in the payment is determined.

[0073] After selection of a credit card, Control unit 310 displays an input screen for a user ID and a password on the display. When the user inputs a user ID and a password, Control unit 310 authenticates the user by the inputted used ID and password (step Sa3). Specifically, Control unit 310 compares a user ID and a password each corresponding to the selected credit card stored in Storage area 233 in EEPROM of UIM 18 with the inputted user ID and password. If the two user IDs and two passwords coincide, Control unit 310 confirms authenticity of the user. If not, it confirms inauthenticity. If the authenticity is confirmed (step Sa3 "NO"), Control unit 310 carries out error processing (step Sa4) for example, displays an error message on the display. If the authenticity is confirmed (step S3 "YES"), Control unit 310 stores the authentication result (authenticity) into Storage area 233 (step Sa5) and outputs the user ID stored in Storage area 233 to Radio interface 370 to transmit to Mobile terminal 17 (step Sa6). Then Control unit 310 terminates processing.

[0074] It is noted that when storing the authentication result into Storage area 233, Control unit 310 may write an expiration time of the authentication result, which is an hour, for example. After the expiration, Control unit 310 deletes the authentication result.

[0075] As a result, a user ID is sent from Portable device 14 to Mobile terminal 17 and subsequently a request for payment is sent from POS terminal to Payment gateway 15 (step S3 in fig.11). Next, an e-mail including commands to execute an application for payment (step S5 in fig.11) is transmitted from Payment gateway 15 to Portable device 14.

[0076] It will now be described that operations of Portable device 14 after reception of the e-mail sent from Payment gateway 15 referring to fig.14. Firstly, Control unit 310 checks whether an e-mail is received (step Sb1).

[0077] If Portable device 14 receives any e-mails, Control unit 310 terminates processing. If Portable device receives e-mail, Control unit 310 determines whether the e-mail is sent from Payment gateway 15 and checks whether the e-mail contains predetermined commands referring to the content of the e-mail (step Sb2).

[0078] If a sender of the e-mail is not Payment gateway 15 or the e-mail does not contain predetermined commands, Control unit 310 terminates the processing. If the sender is Payment gateway 15 and the e-mail contains predetermined commands, Control unit 310 executes an application for payment (step Sb3) before termination.

[0079] Control unit 310 repeats the above series of processes periodically so that the application for payment is executed automatically when receiving an e-mail including the commands.

[0080] It will now be described that operations of Portables device 14 after execution of the application referring to fig. 15.

[0081] Firstly, Control unit 310 reads out from Storage area 233 an address such as Uniform Resource Locator (URL), to access Payment gateway 15 via Mobile communication network 12 (step Sc1). To ensure security, Secure Socket Layer (SSL) is used for data exchange between Portable device 14 and Payment gateway 15.

[0082] To be more specific, when sending a request for access to Payment gateway 15, Portable device 14 requests transmission of an electronic certificate issued by a Certificate Authority (CA) which is not shown in the figure. In response to the request, Payment gateway 15 sends the certificate to be confirmed by Portable device 14. Therefore, Portable device 14 is able to check authenticity of Payment gateway 15, thereby avoiding a danger of communication with an unauthorized server posing as an authorized server. After confirmation of authenticity of Payment gateway 15, data exchange starts. Needles to say, SSL is applied for such data exchange. Since SSL has become a common technique, detailed description is omitted.

[0083] After establishment of the connection between Portable device 14 and Payment gateway 15, Portable device 14 retrieves an authentication result (authenticity), a user ID, and a device ID from Storage area 233. Next, Portable device 14 transmits a request for authentication of the device 14 to Payment gateway 15 via Mobile communication network 12 to request including the retrieved user ID and device ID (step Sc2). At the same time, Control unit 310 measures time (step Sc3). If Portable device 14 does not receive information from Payment gateway 15 in response to the transmission after predetermined time (two minutes, for example), Control unit 310 terminates this processing and performs time-out processing, for example, displaying a message notifying to a user that this payment processing is aborted and must be carried out from the beginning.

[0084] As described before, when Portable device 14 sends an authentication result, a user ID, and a device ID to Payment gateway 15, Payment gateway 15 authenticates confirms the authenticity of the user and device 14. If the authenticity is confirmed, detailed transaction information is sent to Portable device (step S7 and step S8 of fig.11).

[0085] When authenticity is confirmed and thus information on transaction details (name of goods, quantity, price, tax, merchant, for example) is transmitted from Payment gateway 15, Control unit 310 displays the transaction details on the display (step Sc4) to be checked by the user.

[0086] Fig.16 shows an example of a screen on which

APPL-1002
APPLE INC. / Page 389 of 1892

the transaction details is displayed. As shown therein, a name of merchant (shop), a total amount to be paid by the user, and buttons for direction. A user selects one of the buttons of " Agree" and "Not agree" for proceeding or stop paying, respectively. Control unit 310 determines which buttons is selected, in other words, whether the user agrees with this transaction (step Sc5).

[0087] If "Not agree" is selected (step Sc5 "NO"), Control unit 310 stops payment processing (step Sc6). If "Agree" is selected (step Sc5 "YES"), Control unit 310 transmits request for proceeding payment to Payment gateway 15 via Mobile communication network 12 (step Sc7).

[0088] In response to the request for proceeding payment, information on payment methods is transmitted from Payment gateway 15 via Mobile communication network 12, (step Sc9 in fig.11). Upon receipt of the information on payment methods, Control unit 310 displays a list of available payment methods on the display (step Sc8), one of which is to be selected by the user. Fig.17 shows an example of a screen on which the list is displayed. As shown therein, check-boxes each corresponding to each payment method are displayed. A user selects a check-box and "OK" button, to determine a payment method the user would like.

[0089] After the determination, Control unit 310 transmits to Payment gateway 15 via Mobile communication network 12 information for identifying the determined payment method (step Sc9). Upon receipt of the information of payment method, Payment gateway 15 sends a request for credit to Credit server 13. Subsequently, Payment gateway 15 sends a completion message to Portable device 14. Upon receipt of the message, Control unit 310 displays a massage such as " Payment has now been completed." on the display.

B-3. Operations of POS terminal 11

[0090] It will now be described that operations carried out in POS terminal 11 referring to fig. 18. When a user conducts a financial transaction namely, buys goods at a shop, a clerk inputs transaction information including name of goods, quantity, price, and tax into POS terminal (step Sd1) to store the information into storage areas. Control unit then 710 determines whether a user wants to use this electronic payment service (step Sd2).

[0091] If the user doe not want to use this service, or the user pays in cash (step Sd2 "NO"), Control unit 710 performs processing similarly to a general POS terminal (step Sd3). If the user wants to use the service, in other words, the user inputs a request of this service to POS terminal, Control unit 710 accesses Mobile terminal 17 via Interface 740, to determine whether a user ID is received (step Sd4).

[0092] If Mobile terminal 17 has not yet received a user ID sent from Portable device 14 using a short-range radio communication, Control unit 710 repeat accessing periodically until Mobile terminal 17 receives a user ID. When Mobile terminal 17 has received a user ID, Control unit 710 obtains the user ID via Interface 740. Next, Control unit sends to Payment gateway 15 via Communication network 10 a request for transaction number including the transaction information, the merchant information, and the user ID (step Sd5).

[0093] Transaction number is transmitted from Payment gateway 15 to POS terminal 11, in response to the request (step S4 in fig.11). Upon receipt of the transaction number from Payment gateway 15, Control unit 710 stores the received transition number in relation with the transaction information stored in POS terminal earlier (step Sd6).

[0094] After that, Control unit 710 waits for a completion message sent from Payment gateway 15. When receiving a completion message after data exchange between Portable device 14 and Payment gateway 15, Control unit 710 stores the completion message in relation with the transaction information and transaction number (step Sd7) and finally prints out a receipt for the transaction.

B-4. Operations of Payment gateway 15

[0095] It will now be described that operations performed in Payment gateway15 referring to fig. 19. Upon receipt of a request for transaction number from POS terminal 11(step Se1), CPU 151 of Payment server 150 issues a transaction number and sends it to POS terminal 11 via Communication network 10 (step Se2). CPU 151 stores the transaction information, the merchant information, the transaction number, and the date and time included in the request for transaction number into Transaction table 154b (step Se3).

[0096] Next, CPU 151 sends the user ID included in the request for transaction number to Direction server 160 (step Se4). Upon receipt of the user ID sent from Payment server 150, CPU 161 of Direction server 160 generates and stores into a mailbox 164a of the user an e-mail including commands for execution of an application for proceeding payment processing stored and executed in Portable device 14 (step Se5). Next, CPU 161 sends a reception message to Portable device 14 identified by the user ID. When Portable device 14 sends, in response to the message, a request for the e-mail to Direction server 160, CPU 161 sends the e-mail to Portable device 14 (step Se7).

[0097] Upon receipt of the e-mail, Portable device 14 executes the application to make a request for connection with Payment server. CPU151 establishes a connection by using SSL (step Se8). After establishment of the connection, Portable device 14 sends the User ID, authentication result (authenticity of the user), and the device ID to Payment server 150. Payment server 150 checks the authentication result and next authenticates Portable device 14 on the basis of the device ID (step Se9). Specifically, CPU 151 compares the device ID sent from Portable device 14 with a device ID stored in

APPL-1002
APPLE INC. / Page 390 of 1892

relation with the user ID in User table 154a. If the two device IDs coincide, CPU 151 determines authenticity of the device 14 (step Se10).

[0098] If authenticity of the device 14 is not confirmed, namely, the two device IDs do not coincide, CPU 151 sends an error message to Portable device 14 and carries out error processing, for example, stops processing (step Se11). If the authenticity is confirmed, CPU 151 reads out information including transaction details and merchant information stored in Transaction table 154b in step Se3, to send to Portable device 14 via Mobile communication network 12 (step Se12).

[0099] Upon receipt of the above information, Portable device 14 urges the user to confirm the transaction details (step Sc4 and Sc5 in fig.15). If the user agrees with the transaction, a confirmation is transmitted to Payment gateway 15. If the user does not agree, nothing is transmitted. CPU 151 determines whether the confirmation is received within a predetermined time from transmission of the information to Portable device 14 (step Se13). If the confirmation is not received within the time, CPU 151 carries out error processing, for example, stops processing (step Se11).

[0100] If the confirmation is received within the time, CPU 151 determines payment methods available for the transaction and sends information on the payment methods to Portable device 14 via Communication network 12 so that the user can select one among the methods (step Se14). Specifically, CPU 151 refers to User table 154a of fig.7 to specify a credit card number corresponding to the user ID sent from Portable device 14. When the card number is specified, CPU151 refers to Issuer table 154c shown in fig.9 to specify an issuer of the card.

[0101] More specifically, CPU 151 determines within which range the card number lies in 154ca to specify the company. After the company is specified, CPU 151 refers to Merchant table 154d (cf. fig.10), to determine payment methods on the basis of the company and the merchant information included in the request for transaction number sent from POS terminal 11. Suppose that Merchant table 154d shown in fig.10 is stored in HDD 154, that a company "A" whose code number is "2a11111", and that a merchant "A" whose code number is "1111111111". CPU would determine that the user can pay in lump sum, installments, and revolving system and cannot pay with bonus and partially with bonus.

[0102] After transmission of the payment methods to Portable device 14, Portable device 14 sends a payment method to Payment gateway 15. Upon receipt of the payment method, CPU 151 make a request for credit with data in a predetermined format containing the credit card number, the expiration date, the transaction details (name of goods, quantity, price), the merchant information, the payment method, and other related information, to transmit to Credit server 13 via Payment network 16 (step Se15). It is possible that the predetermined format is conventional one used for data exchange between a conventional credit server and a payment device. Finally, CPU 151 terminates processing of the transaction.

[0103] After transmission of the request for credit, CPU 151 waits until a completion message notifying a completion of credit sent from Credit server 13 is received. Upon receipt of the completion message, CPU 151 forwards the completion message to POS terminal via Communication network 10 and to Portable device 14 via Mobile communication network 12 (step Se16).

[0104] As described above, by using the electronic financial transaction service in which a method for electronic payment based on this embodiment is applied, a purchaser don't have to hand his/her credit card in payment to a third-party including a clerk. Furthermore, a purchaser doesn't have to carry a credit card for shopping. Therefore, the danger of card information leakage and possible abuse of cards decreases drastically.

[0105] Also, Portable device 14 authenticates a user at payment, if a third party or other improper person obtains Portable device 14 improperly, the person cannot pay on credit using Portable device 14, thereby preventing the danger of abuse of Portable device 14.

[0106] Since information necessary for payment including a card number and an expiration date is stored in Payment gateway 15, not in Portable device14 or UIM 18, if Portable device 14 or UIM is stolen or improperly obtained, there is little danger of card information leakage from Portable device 14 or UIM. Further, sensitive information such as a card number and expiration date is managed by Payment gateway 15 and cannot provided to public networks such as Mobile communication network 12 and Communication network 10. Therefore, the danger of wiretapping such sensitive information via a public network is reduced.

[0107] In this embodiment, sensitive information necessary for payment is stored in both Portable device 14 and detachable UIM 18. Thus, a user is able to detach UIM from Portable device 14 when it is not required, to prevent the danger of information leakage. Even if such information is leaked, an improper user cannot pay using the device 14 since Payment gateway 15 authenticates Portable device 14 as well a user. In other words, both a user and a portable device are checked.

[0108] In this embodiment, Portable device 14 sends a request for payment to Payment gateway 15 via POS terminal 11; and upon receipt of the request, Payment gateway 15 sends an e-mail to Portable device 14 to obtain a confirmation of transaction from the user. Thus, even if an improper person obtains a user ID and intends to pay using another portable device in combination with the obtained user ID, needless to say, it is the only authorized Portable device 14 that receives the e-mail. Therefore, the improper person does not receive the e-mail and thus is not able to conduct a transaction using the obtained user ID. Namely, the danger of leakage and abuse of a user ID is restricted.

[0109] In the prior art, Payment gateway 15 may sends to Portable device 14 an e-mail including a mes-

APPL-1002
APPLE INC. / Page 391 of 1892

sage like "Please connect with the Payment server for payment", to obtain an instruction of payment from the user. Namely, a user operates Portable device 14 one after another referring to messages. However, in this way, it is often the case that a user forgets operation procedures, or carries out wrong operations. This will cause a problem that a transaction stops or remains uncompleted. On the other hand, in this embodiment, Portable device14 "automatically" executes an application for payment according to commands included in the received e-mail, thereby preventing suspension or stop of payment due to a misoperation made by a user.

[0110] Further, a user is able to register a plurality of credit cards used for the electronic financial transaction service. Specifically, each password is stored in UIM correspondingly to each credit card. As a result, a user is able to select credit cards for use in its appropriate way by inputting each user ID, for example.

[0111] It is noted that a method for payment based on the present embodiment has advantages in a merchant as well in a user described. That is, although a request for transaction number sent from POS terminal 11 to Payment gateway 15 does not contain a card number and expiration date which are send from a POS terminal 1 to a credit server 4 as shown in fig.21 in a conventional system, Payment gateway 15 does contain transaction details and a merchant information used in a conventional system. Therefore, a merchant can participate in this transaction service simply by making, at POS terminal 11, a data including information necessary for a transaction in a conventional format and sending it to Payment gateway 15. This provides benefits to a merchant because the merchant does not have to install a new POS terminal.

[0112] Further, Credit server 13 performs processing in the conventional way because Payment gateway sends a request for credit in a conventional format to Credit sever 13. This provides convenience to a credit company because the company does not have to install a new server.

[0113] Since Transaction table 154b stores transaction details conducted by a user, it is possible that Payment gateway collectively manages electronic records on payments (so called electronic receipt). In a conventional credit payment system, generally, a merchant issues a payment voucher on which transaction details are entered and mails it to a depository for managing payment vouchers provided by an issuer. However in this embodiment, Payment gateway 15 is able to manage payment information collectively, thus the cost of issuing and managing payment vouchers can be reduced.

C. Modification of the first embodiment

[0114] The present invention is susceptible to many modifications as follows.

[0115] In the above embodiment, Storage area 233 of UIM 18 stores a device ID for identifying Portable device 14 used for the electronic financial transaction service. Portable device14 transmits the device ID to Payment gateway 15 and Payment gateway 15 compares the transmitted device ID and a device ID stored in User table 154a for authentication of the device 14. However, it is possible that the authentication is carried out using SSL, for example. In this case, Portable device 14 sends to Payment gateway 15 a digital certificate for client authentication which has been registered at Certificate Authority (CA). Payment gateway 15 authenticates a device using the certificate.

[0116] In the above embodiment, Portable device 14 urges a user to input a user ID and a password for a user authentication. However, it is possible to use biometrics such as fingerprint, iris scan, or combined voice and face patterns for the authentication.

[0117] In the above embodiment, a user ID is transmitted to POS terminal 11 via Mobile terminal 17 when the user conducts a financial transaction at a shop. However, the present invention is not only applied to such an actual shop but can be applied to an online shopping via Internet, for example. An example of such applications is shown in fig.20 in which a Web server 130 is provided instead of POS terminal 11 and Mobile terminal 17.

[0118] Web server 130, so called an online shop server, receives a request for purchase from terminals including a personal computer and a mobile phone with features of Web browsing. To be more specific, when user selects or inputs a URL for connection with the Web server 130, a web page for selection of goods is displayed on the terminal. The user makes a request for purchase seeing the page and sends it to Web server 130. A method of the present invention can be applied to procedures used for such a system for payment.

[0119] Specifically, firstly Portable device14 authenticates a user. If authenticity is confirmed, a user ID is transmitted from Portable device 14 to Web server 130 via Mobile communication network 12 and a Communication network 10A. Upon receipt of the user ID, Web server 130, instead of POS terminal 11, sends a request for transaction number including transaction information, the user ID, and merchant information. Next, payment processing is performed among Portable device 14, Payment gateway 15, and Credit server 13 similarly to the first embodiment. After completion of the payment processing, a completion message is sent from Payment gateway 15 to Web server 130 via Communication network 10A.

[0120] In the first embodiment, transaction information conducted by a user is stored in Transaction table 154b. Thus, it is possible that a user checks transaction information of the user with Portable device 14, personal computer, or a mobile phone with features including Web browsing. Specifically, when receiving a request for the check from a terminal via Internet, Payment gateway 15 retrieves the transaction information form table

APPL-1002
APPLE INC. / Page 392 of 1892

154b and transforms it into a HTML format for transmission to the terminal.

[0121] In the first embodiment, information necessary for payment is stored in EEPROM 230 of detachable UIM 18 to be read out by Control unit 310. However, it is possible that a memory such as an EEPROM incorporated into Portable device 14 stores such information instead of UIM 18.

[0122] Further, a module such as an IC chip having high resistance to tampering in which information for payment including a user ID and a password is stored and read out by Control unit can be used instead of UIM 18. Needless to say, such a module can be mounted detachably.

[0123] In the first embodiment, a purchaser uses Portable device capable of communicating with Payment gateway by radio via Mobile communication network 12 for electronic payment. However, a personal computer can be used as a terminal for payment in the system, for example. Specifically, such a computer is connected with Internet via a fix telephone network and has an input device, display, and other devices necessary for the electronic payment.

[0124] In the first embodiment, a user ID is transmitted via Mobile terminal 17 to POS terminal 11. However, if POS terminal 11 features Bluetooth for data exchange, Portable device 14 may transmit directly to POS terminal 11. It is possible that a user ID can be transmitted from Portable device 14 to POS terminal 11 using other commutation methods.

[0125] In the first embodiment, data exchange is carried out between POS terminal 11 and Payment gateway 15 via Communication network 10. It is possible that Mobile terminal 17 is connected with Communication network 10 to exchange data between POS terminal 11 and Payment gateway via Mobile terminal 17 and Communication network 10.

[0126] In the first embodiment it is possible that if a user uses two or more credit cards for the electronic transaction system, a user ID or a password is assigned to the cards. In this case, before selection of credit card (step Sa1 of fig.12), a user may input the user ID and a password before Portable device 14 authenticates the user. After the authentication, credit cards corresponding to the user ID and the password are displayed. Then the user selects one among the cards.

[0127] In the first embodiment, Control unit 310 executes application programs in data exchange between POS terminal and Payment gateway 11 and authentication of a user and a device 14. It is possible that a storage medium such as a CD-ROM or a floppy disk in which such programs for the electronic payment is stored is provided to users. The programs may be provided via Internet.

(Second embodiment)

[0128] A second embodiment of the present invention will now be described referring to the drawings.

D. Configuration of the system

D-1. Overall configuration

[0129] Fig.22 shows an electronic payment system using a method for electronic paying based on the second embodiment of the present invention.

[0130] As shown, Electronic payment system 15A has a POS terminal 11A and Credit server 13A. Payment gateway 15A is connected with Terminal 11A and Credit server 13A via a dedicated line (not shown) for data exchange. Terminal 11A and Payment gateway may be connected via a public network. Payment gateway 15A is also connected to Portable device 14A.

D-2. POS terminal

[0131] POS terminal 11A has a storage unit such as a hard drive and an input device such as a keyboard, a mouse or a card reader, in addition to Display, Control unit including a CPU, ROM, RAM, and a communication interface same as POS terminal 11 of the first embodiment. Fig.23 shows an example of information stored in the storage. As shown, "issuer code", "payment method", and "merchant code" are stored correspondingly. The "issuer code" identifies an issuer (credit card company) of a credit card by which a user can pay at a shop where POS terminal 11A is installed. The "payment method" is a payment method available for a purchaser at the shop such as a lump sum, installments, or with bonus. The "merchant code" identifies a shop of a merchant.

D-3. Credit server

[0132] Credit server 13A includes a CPU, a RAM, a ROM, an input device such as keyboard or mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem.

[0133] Figs.24A through 24D shows an example of information stored in the storage unit of Credit server 13A. Fig.24A shows information relating to POS terminal 11A. Specifically, "merchant code for credit", "payment method", and "merchant code" are stored correspondingly. The "merchant code for credit" allows an issuer (credit company) to identify a merchant or a shop with which a transaction is conducted. It may be an ID number of a shop or of POS terminal 11A.

[0134] Fig.24B shows information relating to users of credit cards. Specifically, "user name", "user address", "card number", " expiration", and "credit limit" are stored correspondingly.

[0135] Fig.24C shows an example of histories of transactions conducted by users. " Card number", "decryption key", "type", "date", "transaction number", "merchant number"," amount", "payment method", and

APPL-1002
APPLE INC. / Page 393 of 1892

" merchandise code" are stored correspondingly. Information stored in "card number" in fig.24C is same as stored in fig.24B. In fig.24C it is permitted that a card number is stored for several times because a user may conduct transactions several time with the card.

[0136] The "decryption key" is used for decrypting an encrypted card number which is sent from Payment gateway 15A to POS terminal 11A. The "type" represents types of transactions. The "date" represents date of payment. The " transaction number" is a serial number each assigned to a transaction. The "merchant number" identifies a shop of a merchant with which a transaction is conducted. The "amount" represents a price of merchandise (possibly including tax). The "payment method" represents payment in a lump sum, or installments, for example. The "merchandise code" identifies merchandise transacted.

[0137] Fig.24D shows an example of information on transaction details conducted at each shop. Specifically, "merchant number", " type", "date", "sales", "card number", and "payment method" are stored. Information stored in "merchant number", "type", and "date" is same as stored in fig. 24C. The "sales" represents a price of merchandise, which is same as "amount" in fig.24C if tax is not included in the "amount". The "payment method" represents a payment method selected by a user.

D-4. Portable device

[0138] Portable devicel4A is, for example, a cellular phone capable of carrying out data communications. To be more specific, it may use (Personal Digital Cellular (PDC) of Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), or any other schemes for data communication. Further, Third generation (3G) scheme such as IMT-2000 may be applied. Needles to say, PDA and other portable devices can be applied.

D-5. Payment gateway

[0139] Payment gateway 15A includes a CPU, a RAM, a ROM, an input device such as a keyboard or a mouse, a display, a storage unit such as a hard drive, and a communication interface such as a modem. Functionally, Payment gateway 15A comprises a receiving unit 101, a checking unit 102, encryption unit 103, a number transmitting unit 104, a key generation unit 105, a key transmitting unit 106, a transmitting/receiving unit 107, a notifying unit 108, and a storage unit 109.

[0140] Transaction unit 101 receives a user ID to identify a user assigned to the user in advance and a merchant code to identify a shop, which is sent from POS terminal 11A where the user conducts a transaction. Upon receipt of a user ID and a merchant code, Receiving unit 101 transfers the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0141] Checking unit 102 retrieves a card number of a user from Storage unit 109 on the basis of a user ID received by Receiving unit 101. Specifically, Checking unit 102 retrieves a from Storage unit 109 a card number and an issuer code corresponding to a user ID received by Receiving unit 101. Checking unit 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. If the user ID is not found or the expiration date has passed, Checking unit 102 outputs to Notifying unit 108 a message notifying failure of authentication.

[0142] Figs.25A and 25B show an example of information stored in Storage unit 109. As shown in Fig.25A, information relating to shops which participate in the electronic payment service provided by Payment gateway 15A is stored. To be more specific, a merchant codes and corresponding shop name.

[0143] Fig.25B shows an example of information relating to users. Specifically, user IDs and corresponding passwords, user names, phone numbers, e-mail addresses, terminal numbers, card numbers, issuer codes, and expirations are stored correspondingly. The password is used for authentication of a user.

[0144] The phone number is a telephone number of portable device 14A. The e-mail address is an e-mail address for Portable device 14A. The device number is, for example, a serial number assigned for each Mobile station 14A, which identifies Mobile station 14A. The card number is a number of a credit card by which a user pays. A user registers the card number to Payment gateway 15A in advance. The issuer code identifies an issuer of a card (credit company). The expiration represents an expiration date of the credit card.

[0145] Encryption unit 103 encrypts a card number obtained by Checking unit 102, to generate a "encrypted card number". Specifically, Checking unit 103 encrypts a card number, in a way that it can be decrypted using an encryption key generated by Key generating unit 105. Suppose that the decryption key is "0123", that the card number is "3456", and that the encryption calculation is an addition, the encrypted card number becomes "3579". In decryption, "0123" is subtracted from "3579" to be generated the card number "3456". Encryption unit 103 outputs to Key generating unit 105 a card number, its encrypted card number, and an issuer code. Further, Encryption unit 103 outputs to Number transmitting unit 104 the encrypted card number and the merchant code.

[0146] Number transmitting unit 104 transmits an encrypted card number made by Encryption unit 103 to POS terminal 11A specified by the merchant code obtained from Encryption unit 103.

[0147] Key generating unit 105 generates a decryption key used for decryption of a card number. In this embodiment, a card number is encrypted by Encryption unit 103 using a decryption key. It is possible that the decryption key is generated using both the decryption key and the card number. Key generating unit 105 outputs to Key transmitting unit 106 the encrypted card umber, the decryption key, and the issuer code.

APPL-1002
APPLE INC. / Page 394 of 1892

[0148] Key transmitting unit 106 transmits to Credit server 13A an encrypted key generated by Key generating unit 105. Specifically, Key transmitting unit 106 transmits, to Credit server by a credit company specified by the issuer code provided form Key generating unit 105, the encrypted card number and the decryption key.

[0149] When Receiving unit 101 receives a user ID, Transmitting/receiving unit 107 transmits to portable device 14A a confirmation e-mail including transaction details. If Portable device 14A does not reply to the e-mail, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106, to cancel the transaction conducted on the basis of the user ID.

[0150] To be more specific, Transmitting/receiving unit 107 retrieves from Storage unit 109 an e-mail address on the basis of the user ID provided from Receiving unit 101. Transmitting/receiving unit 107 then transmits a confirmation e-mail including transaction details to Portable device 14A specified by the e-mail address. Upon receipt of a reply e-mail from Portable device 14A, Transmitting/receiving unit 107 checks a password included in the reply e-mail against a password stored in Storage unit 109, to authenticate the user.

[0151] If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106, to cancel the transaction conducted on the basis of the user ID. A method for obtaining a confirmation from a user is not limited to the e-mail. For example, Transmitting/receiving unit 107 can transmit to Portable device14A a reception message which is generally used for cellular phone. It is possible that, in the authentication of a user, Transmitting/receiving unit 107 uses, in addition to a password, information to identify Portable device 14A uniquely such as a device ID.

[0152] If Checking unit 102 does not find the credit card corresponding to the user ID in Storage unit 109, Notifying unit 108 notifies POS terminal 11A of failure of authentication.

E. Operations of the system

[0153] Detailed procedures for payment processing in an electronic financial transaction system based on the second embodiment will now be described referring to figs. 26 and 27.

[0154] As shown in fig.26, firstly, POS terminal 11A obtains a user ID from a user and transmits the user ID and a merchant code to Payment gateway 15A (step S01). Specifically, a user inputs a user ID with the input device of POS terminal, for example. POS terminal 11A may obtain the user ID from Portable device 14A. Receiving unit 101 receives the user ID and the merchant code (step S02). Next, Receiving unit 101forwards the user ID and the merchant code to Checking unit 102 and Transmitting/receiving unit 107.

[0155] Upon receipt of the user ID, Transmitting/receiving unit 107 sends a confirmation e-mail to Portable device 14A corresponding to the user ID (step S03). After the sending, Transmitting/receiving unit 107 is ready for receiving reply e-mail (step S04). If Transmitting/receiving unit 107 does not receive a reply e-mail or the both passwords does not agree, Transmitting/receiving unit 107 stops at least one of Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, and Key transmitting unit 106, to cancel the transaction conducted on the basis of the user ID (step S05).

[0156] When Transmitting/receiving unit 107 receives the reply e-mail, Checking unit 102 retrieves from Storage unit 109 a card number stored correspondingly to the user ID provided from Receiving unit 101 (step S06). It is noted that steps S03 and S04 can be omitted.

[0157] Checking unit 102 checks the card number retrieved from Storage unit 109 against the card number provided from Receiving unit 101 (step S07). If the user ID is not found in Storage unit 109 or the expiration date has passed, Checking unit 102 notifies Notifying unit 108 of failure of authentication.

[0158] Upon receipt of the message from send from Checking unit 102, Notifying unit 108 sends a message notifying POS terminal of failure of authentication (step S08). POS terminal 11A receives the message to be notified the user (step S09).

[0159] If the credit card number corresponding to the user ID is retrieved form Storage unit 109 in step S07, Checking 102 outputs the card number, the issuer code, and the merchant code to Encryption unit 103. When Encryption unit 103 receives the card number, the issuer code, and the merchant code, Key generating unit 105 generates a decryption key used for decryption of an encrypted card number (step S10). Key generating unit 105 outputs the key to Encryption unit 103 to obtain the card number and the issuer code. Next, Key generating unit 105 sends to Key transmitting unit 106 the card number and the issuer code along with the key.

[0160] Upon receipt of the decryption key from Key generating unit 105, Encryption unit 103 encrypts the card number in a way that the encrypted card number is decrypted with the decryption key (step S11). Next, Encryption unit 103 outputs the encrypted card number and the merchant code to Number transmitting unit 104.

[0161] Referring to fig.27, Number transmitting unit 104 transmits the encrypted card number to POS terminal 11A indicated by the merchant code (step S12). Key transmitting unit 106 transmits the encrypted card number and the key to Credit server 13A indicated by the issuer code (step S13). The encryption key may be generated for each user, or for each credit company. In case a common key is used as the decryption key for this system, Key transmitting unit 106 does not necessarily transmit the key to Credit server 13A more than

APPL-1002
APPLE INC. / Page 395 of 1892

twice. But needless to say, when the key is updated, Key transmitting unit 106 transmits the updated key. Upon receipt of the encrypted card number and the decryption key, Credit server 13A stores the number and the key into a storage unit of Credit server 13A (step S14).

[0162] POS terminal 11A receives and stores into a storage unit of POS terminal 11A the encrypted card number (step S15). Next, POS terminal 11A makes a request for credit to transmit to Credit server 13A (step S16). Specifically, the request includes, a type, date, transaction number, merchant code for credit, amount, payment method, merchant code as described above, in addition to the encrypted card number.

[0163] Upon receipt of the request (step S17), Credit server 13A determines whether the request is accepted referring to the encrypted card number (step S18). Specifically, Credit server 13A checks the encrypted card number and the decryption key which has already been transmitted by Payment gateway 15A against the decryption key transmitted by POS terminal 11A. If both keys coincide, Credit server 13A decrypts the encrypted card number using corresponding decryption key which has already been received from Payment gateway 15A. If the encrypted card number is not found, Credit server 13A sends a message notifying a failure of authentication to POS terminal 11A to be provided to the user (step S19). POS terminal 11A receives the message (step S20). If the encrypted card number is found, Credit server 13A sends an allowance message (step S21). POS terminal 11A receives the message to be provided to the user.

[0164] A payment program 92 for making a computer to function as Payment gateway 15A and a storage medium 9 will now be described referring to fig.28. Fig.28 shows a functional structure of the storage medium. Storage media 9 is, for example, a magnetic disk, an optical disk including a CR-ROM, or a semiconductor memory.

[0165] As shown in fig.9, Storage medium 9 has a program area 91 and a data area 93. Data area stores a database 931 same as Storage unit 109 shown in fig.22.

[0166] Program area 91 stores Payment program 92. Payment program 92 includes a main module 921 for controlling the following modules, a module 922 for receiving transaction information, a module 923 for checking a card number, a module 924 for encrypting a card number, a module 925 for transmitting an encrypted card number, a module 926 for generating a decryption key, a module 927 for transmitting a decryption key, a module 928 for transmitting a confirmation message and receiving a reply message, and a module 929 for notifying a message of failure of authentication. These modules 922 through 929 have same functions as the Receiving unit 101, Checking unit 102, Encryption unit 103, Number transmitting unit 104, Key generating unit 105, Key transmitting unit 106, Transmitting/receiving unit 107, Notifying unit 108, respectively.

[0167] In the second embodiment, since the encrypted card number is transmitted from Payment gateway to POS terminal 11A and the encrypted card number is generated by Payment gateway 15A on the basis of a user ID transmitted from POS terminal, a merchant cannot obtain a card number. Therefore, security of transaction is ensured in this system. In other words, a user is able to send a card number safely to Payment gateway 15A to conduct a transaction. Payment gateway transmits a decryption key to Credit server 13A, thus Credit server 13A obtains a decryption key corresponding to the encrypted card number. Therefore, Credit server 13A is able to determine whether a request for credit should be accepted using an encrypted card number and corresponding decryption key. Furthermore, an encrypted card number is generated each time a transaction is conducted, thus a merchant can manage sales at the shop, not knowing a card number.

[0168] In this embodiment, when Payment gateway 15A does not receive a reply mail from Portable device 14A, payment processing related to the user ID is stopped. Therefore, if an authorized person obtains a user ID improperly, the person cannot conduct any transactions using the user ID.

[0169] If Payment gateway 102 cannot find a card number corresponding to a user ID, Payment gateway 102 transmits a message notifying failure of authentication to POS terminal 11A, thus a merchant and a user can recognize that the card is not available for the transaction.

Claims

1. An electronic payment method comprising the steps of:

   authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;

   storing an authentication result of said user, by said user terminal, when said user terminal confirms authenticity of said user;

   transmitting a user identification information stored beforehand in said user terminal to a merchant terminal when said user terminal confirms authenticity of said user, by said user terminal;

   transmitting to payment device via a first communication network said user identification information and transaction information transmitted from said user terminal, by said merchant terminal;

   receiving said user identification information and said transaction information transmitted from said merchant terminal, by said payment device;

   identifying said user terminal on the basis of

APPL-1002
APPLE INC. / Page 396 of 1892

said user identification information and transmitting commands for instructing transmission of said authentication result to said user terminal via a second communication network;
transmitting authenticity of said user to said payment device via said second communication network if said user terminal stores authenticity of said user, by said user terminal; and
performing payment processing on the basis of said transaction information upon receipt of said authenticity from said user terminal, by said payment device.

2. The method of claim 1, further comprising the steps of:

transmitting said transaction information to said user terminal via said second communication network upon receipt of said authenticity of said user from said user terminal, by said payment device;
receiving said transaction information transmitted from said payment device and notifying said user of said transaction information, to be checked by said user, by said user terminal; and
when said user inputs an instruction for proceeding payment processing to said user terminal, transmitting to said payment device a request for proceeding payment processing; and
wherein upon receipt of said request, said payment device performs payment processing on the basis of said transaction information.

3. The method of claim **1**, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal along with said authentication result;
said payment device authenticates said user terminal referring to said terminal identification information; and
when authenticity of said user terminal is confirmed, said payment device performs payment processing on the basis of said transaction information.

4. The method of claim **1**, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

5. The method of claim 1, wherein upon receipt of said authenticity from said user terminal, said payment device retrieves a card number and an expiration date on the basis of said user identification information and sends a request for credit including the card number and the expiration date to a credit server provided by a credit company.

6. An electronic payment method comprising the steps of:

authenticating a user of a user terminal on the basis of user identification information inputted to said user terminal by said user, by said user terminal;
transmitting user identification information for identifying a user to a merchant terminal, by said user terminal, when said user terminal confirms authenticity of said user;
transmitting to a payment device via a first commutation network said user identification information transmitted from said user terminal, by said merchant terminal;
receiving said user identification information from said merchant terminal, by said payment device;
identifying said user terminal referring to received user identification information and transmitting commands for executing an application for payment stored in said user terminal to identified user terminal via a second communication network, by said payment device;
upon receipt of said commands, executing said application to transmit a request for proceeding payment processing to said payment device via said second communication network, by said user; and
upon receipt of said request from said user terminal, performing a payment processing.

7. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user of said user terminal on the basis of user identification information inputted to said user terminal by said user; if authenticity of said user is confirmed, stores authentication result; and
transmits to said merchant terminal user identification information stored in said user terminal;
said merchant terminal transmits to said payment device via said first communication network said user identification information transmitted from said user terminal and transaction information;
said payment device identifies said user terminal on the basis of said user identification information transmitted from said merchant terminal and
transmits to said identified user terminal via said second communication network commands for instructing transmission of said au-

APPL-1002
APPLE INC. / Page 397 of 1892

thentication result;
said user terminal transmits to said payment device via said second communication network according to said commands transmitted from said payment device when said user terminal stores said authentication result; and
upon receipt of said authentication result from said user terminal, said payment device performs payment processing on the basis of said transaction information.

8. The system of claim 7, wherein after reception of said authentication result from said user terminal, said payment device transmits said transaction information to said user terminal via said second communication network;
said user terminal receives said transaction information form said payment device;
notifies said user of said transaction information to be checked by said user; and
if said user inputs to said user terminal an instruction of proceeding a payment processing, transmits a request for proceeding payment processing to said payment device via said first communication network; and
upon receipt of said request, said payment device performs payment processing.

9. The system of claim 8, wherein said user terminal transmits to said payment device terminal identification information for identifying said user terminal stored in said user terminal along with said authentication result; and
said payment device authenticates said user terminal on the basis of said terminal identification information;
if authenticity of said user terminal is confirmed, performs payment processing on the basis of said transaction information.

10. The system of claim 7, wherein a detachable storage medium for storing said user identification information is mounted to said user terminal; and
when said user terminal confirms authenticity of said user on the basis of said user identification information, said user terminal transmits to said merchant terminal said user identification information stored in said storage medium.

11. The system of claim 7, wherein said second communication network is a mobile communication network and said user terminal is a mobile station.

12. The system of claim 7, wherein when receiving said authentication result from said user terminal, said payment device retrieves a card number and an expiration on the basis of said user identification information and sends a request for credit including said card number and said expiration to a credit server managed by a credit company.

13. An electronic payment system having a payment device, a merchant terminal connected with said payment device via a first communication network, and a user terminal connected with said payment device via a second communication network **characterized in that**:

said user terminal authenticates a user on the basis of said user identification information inputted to said user terminal by said user;
if authenticity of said user is confirmed, transmits to said merchant terminal a user identification information for identifying said user;
said merchant terminal transfers said user identification information to said payment device via said first communication network;
said payment device identifies said user terminal on the basis of said user identification information and transmits to said identified user terminal via said second communication network commands for executing an application for payment stored in the user terminal;
said user terminal executes said application according to said commands and transmits a request for proceeding payment processing to said payment device via said second communication network; and
said payment device performs said payment processing according to said request.

14. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a storing means for storing an authentication result when authenticity of said user is confirmed by said authenticating means;
a storage medium for storing said user identification information;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
a receiving means for receiving commands for instructing transmission of said authentication result which is transmitted, in response to said

APPL-1002
APPLE INC. / Page 398 of 1892

request for payment, from said payment device via said second communication network; and
a second transmitting means for transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

15. The user terminal of claim 14, wherein said storage medium further stores a terminal identification information for identifying said user terminal; and
said second transmitting means transmits, along with said authentication results, said terminal identification information stored in said storage medium to said payment device via said second communication network.

16. The user terminal of claims 14 or 15, wherein said storage medium is mounted detachably to said user terminal; and
said first transmitting means transmits to said merchant terminal said user identification information stored in said storage medium, when authenticity of said user is confirmed by said authenticating means on the basis of said user identification information.

17. The user terminal of claim 14 or 15, wherein said second communication network is a mobile communication network; and
said user terminal further comprises a radio communication means for exchanging data via said mobile communication network.

18. A user terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network, comprising:

an authenticating means for authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user;
a first transmitting means for transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information
a receiving means for receiving commands for executing an application for payment which is transmitted from said payment device via said second communication network; and
a second transmitting means for executing said application for payment stored in said user terminal and transmitting, according to said application, a request for proceeding payment processing to said payment device via said second communication network.

19. A payment device comprising:

a receiver for receiving a request for payment including a user identification information for identifying a user of a user terminal from a merchant terminal via a first communication network;
an identifying means for identifying said user terminal among registered user terminal on the basis of said received user identification information; a transmitter for transmitting to said identified user terminal via a second communication network commands for executing an application for payment stored in the user terminal; and
a processing means for performing a payment processing on the basis of a request sent from the user terminal via said second communication network after transmission of said commands.

20. A computer program product for making a computer incorporated into a communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

21. A storage medium for storing a computer program product for making a computer incorporated into a

APPL-1002
APPLE INC. / Page 399 of 1892

communication terminal used for an electronic payment system having a payment device connected with a first and a second communication network and a merchant terminal connected with said payment device via a first communication network to execute the steps of:

authenticating a user of said communication terminal on the basis of a user identification information inputted to said user terminal by said user; storing an authentication result into a storage means when authenticity of said user is confirmed by said authenticating means;
transmitting, when authenticity of said user is confirmed, said user identification information stored in said storage means to said merchant terminal so that said merchant terminal transmits to said payment device a request for payment processing including said user identification information;
receiving commands for instructing transmission of said authentication result which is transmitted, in response to said request for payment, from said payment device via said second communication network; and
transmitting, upon receipt of said commands, a request for proceeding said payment processing including said authentication result to said payment device via said second communication network.

22. A payment device comprising:

a storage unit for storing a user identification information for identifying a user of a user terminal and a card number of a credit card correspondingly; a receiving unit for receiving from a merchant terminal a user identification information;
a retrieving unit for retrieving from said storage unit a card number corresponding to said identified user;
an encrypting unit for encrypting the retrieved card number;
a generating unit for generating a key for decryption of said encrypted card number;
a first transmitting unit for transmitting to said merchant terminal said encrypted card number; and
a second transmitting unit for transmitting said key to a credit server managed by an issuer of the credit card.

23. The payment device of claim 22, further comprising a confirming means for transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

24. The payment device of claim 22 or 23, further comprising a notifying means for transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

25. An electronic payment method comprising the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal, by a receiving unit;
retrieving from a storage unit a card number corresponding to said identified user, by a retrieving unit;
encrypting the retrieved card number, by an encrypting unit;
generating a key for decryption of said encrypted card number, by a generating unit;
transmitting to said merchant terminal said encrypted card number, by a first transmitting unit; and
transmitting said key to a credit server managed by an issuer of the credit card, by a second transmitting unit.

26. The electronic payment method of claim 25, further comprising the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information, by a confirming means.

27. The electronic payment method of claim 25 or 26, further comprising the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit, by a notifying means.

28. A computer program product for making a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;

APPL-1002
APPLE INC. / Page 400 of 1892

retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

29. The computer program product of claim 28, for making said computer to further execute the step of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

30. The computer program product of claim 28 or 29, for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

31. A computer readable storage medium for storing a computer program product for making a computer to execute the steps of:

receiving from a merchant terminal a user identification information for identifying a user of a user terminal;
retrieving from a storage unit a card number corresponding to said identified user;
encrypting the retrieved card number;
generating a key for decryption of said encrypted card number; transmitting to said merchant terminal said encrypted card number; and
transmitting said key to a credit server managed by an issuer of the credit card.

32. The storage medium of claim 31, for storing a computer program product for making said computer to further execute the steps of transmitting, when said receiving means receives said user identification, information said receiving unit transaction information to said user terminal and if confirmation of said transaction information form said user terminal is not received, stopping processing performed by any of said a receiving unit, an encrypting unit, a generating unit, a first transmitting unit, and a second transmitting unit, to terminate payment processing corresponding to the user identification information.

33. The storage medium of claim 31 or 32, for storing a computer program product for making said computer to further execute the step of transmitting to said merchant terminal a rejection message if the card number is not stored in said storage unit.

APPL-1002
APPLE INC. / Page 401 of 1892

FIG. 1

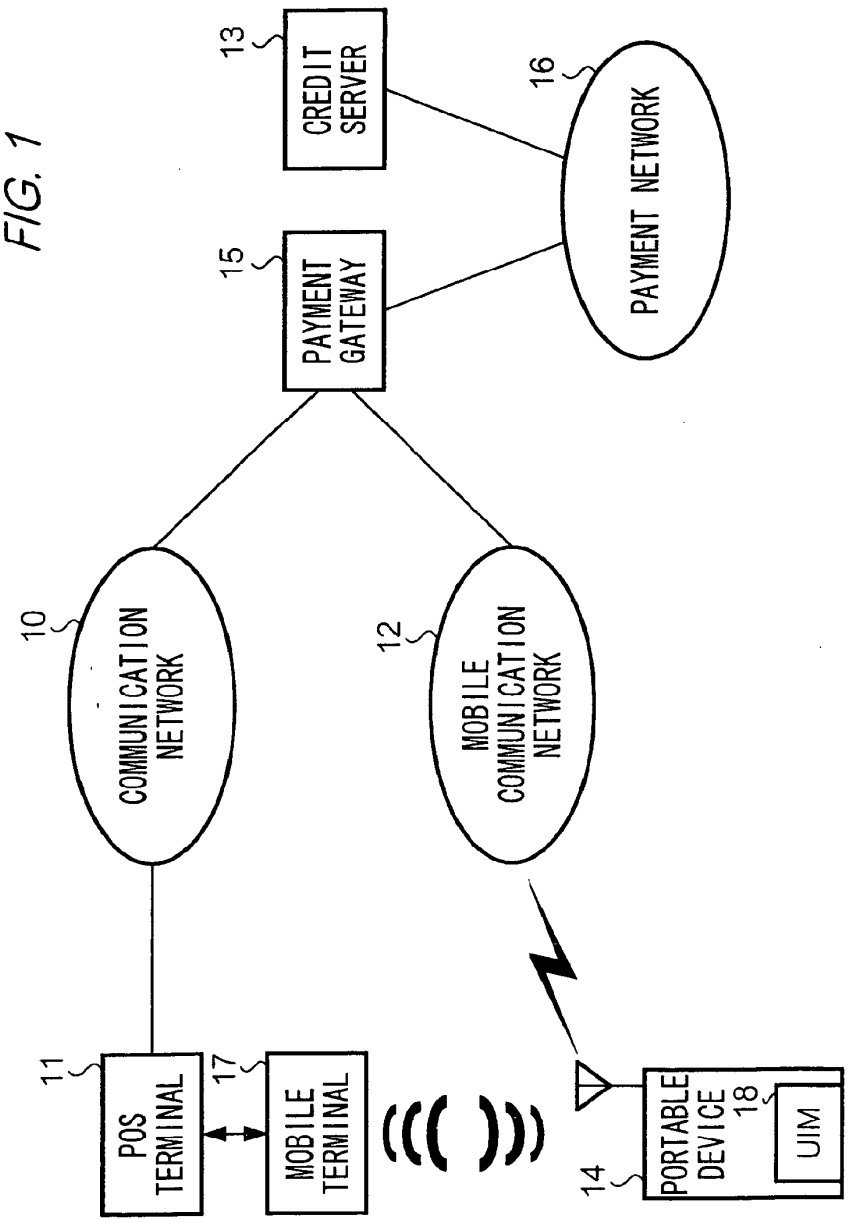

13
CREDIT SERVER
16
PAYMENT NETWORK
15
PAYMENT GATEWAY
10
COMMUNICATION NETWORK
12
MOBILE COMMUNICATION NETWORK
11
POS TERMINAL
17
MOBILE TERMINAL
14
PORTABLE DEVICE
18
UIM

FIG. 2

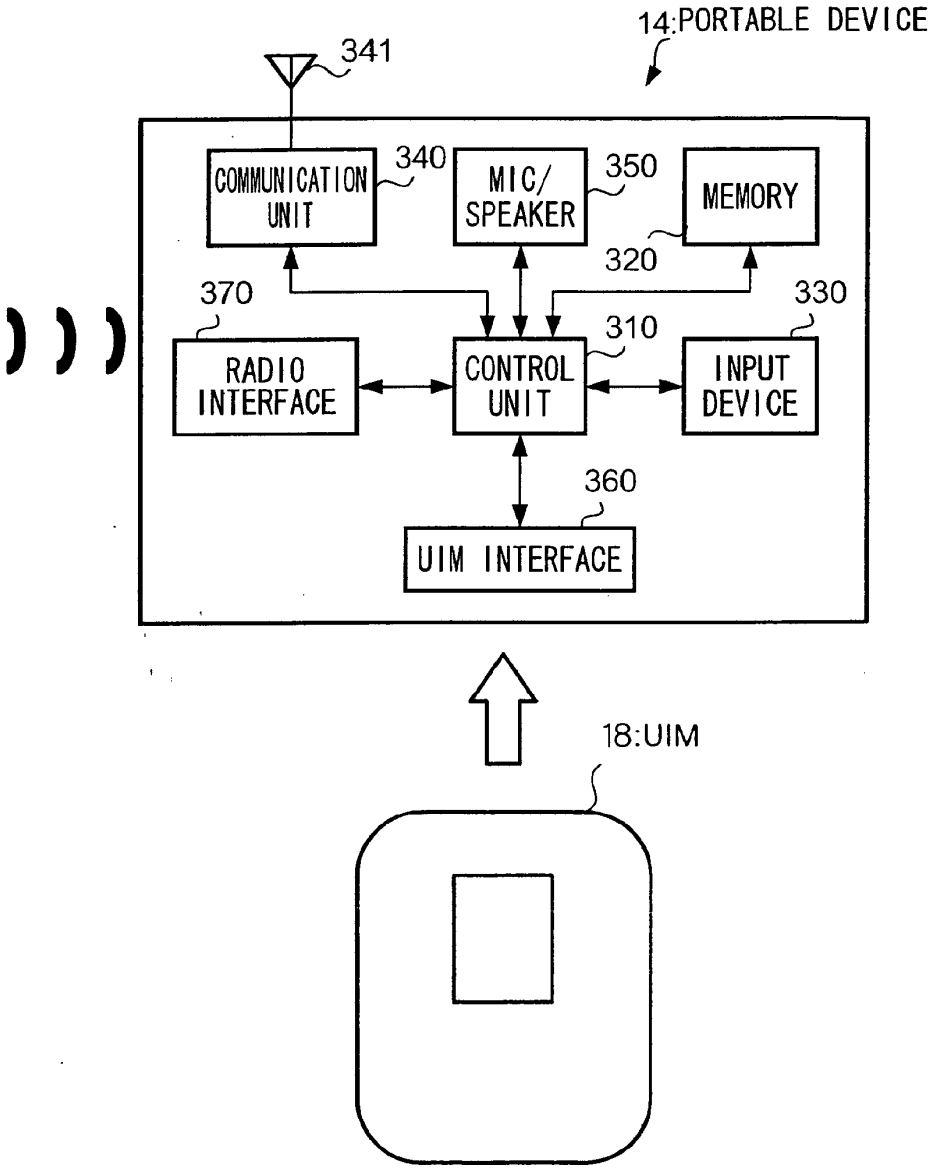

14:PORTABLE DEVICE
341
COMMUNICATION UNIT
340
MIC/ SPEAKER
350
MEMORY
320
370
330
310
RADIO INTERFACE
CONTROL UNIT
INPUT DEVICE
360
UIM INTERFACE
18:UIM

FIG. 3

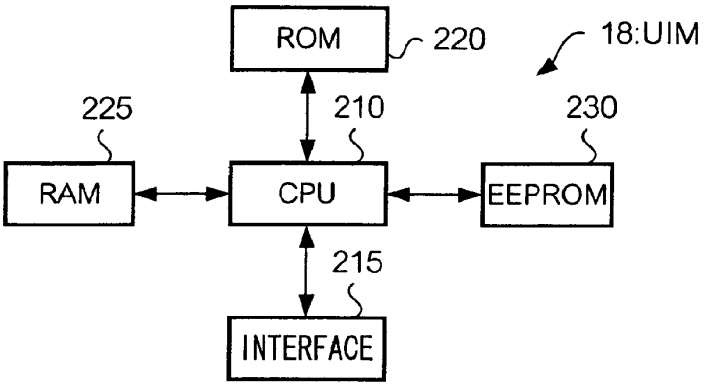
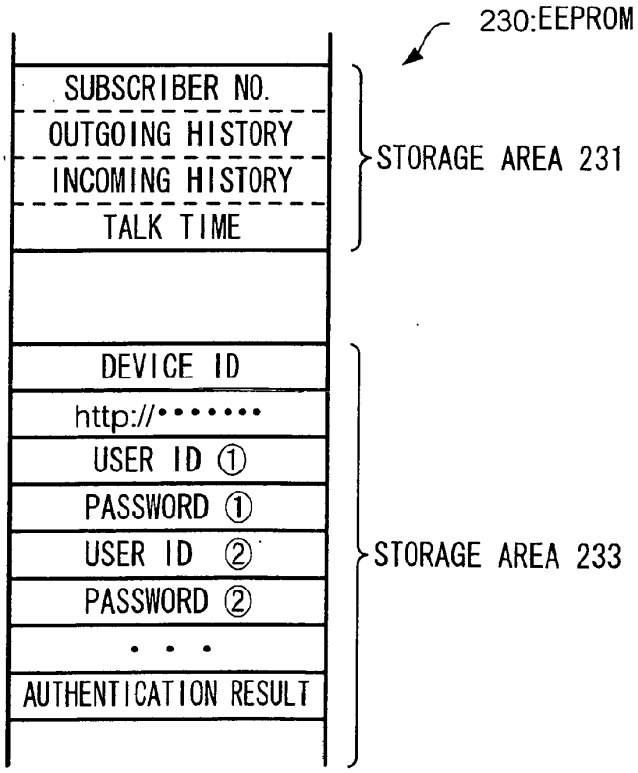
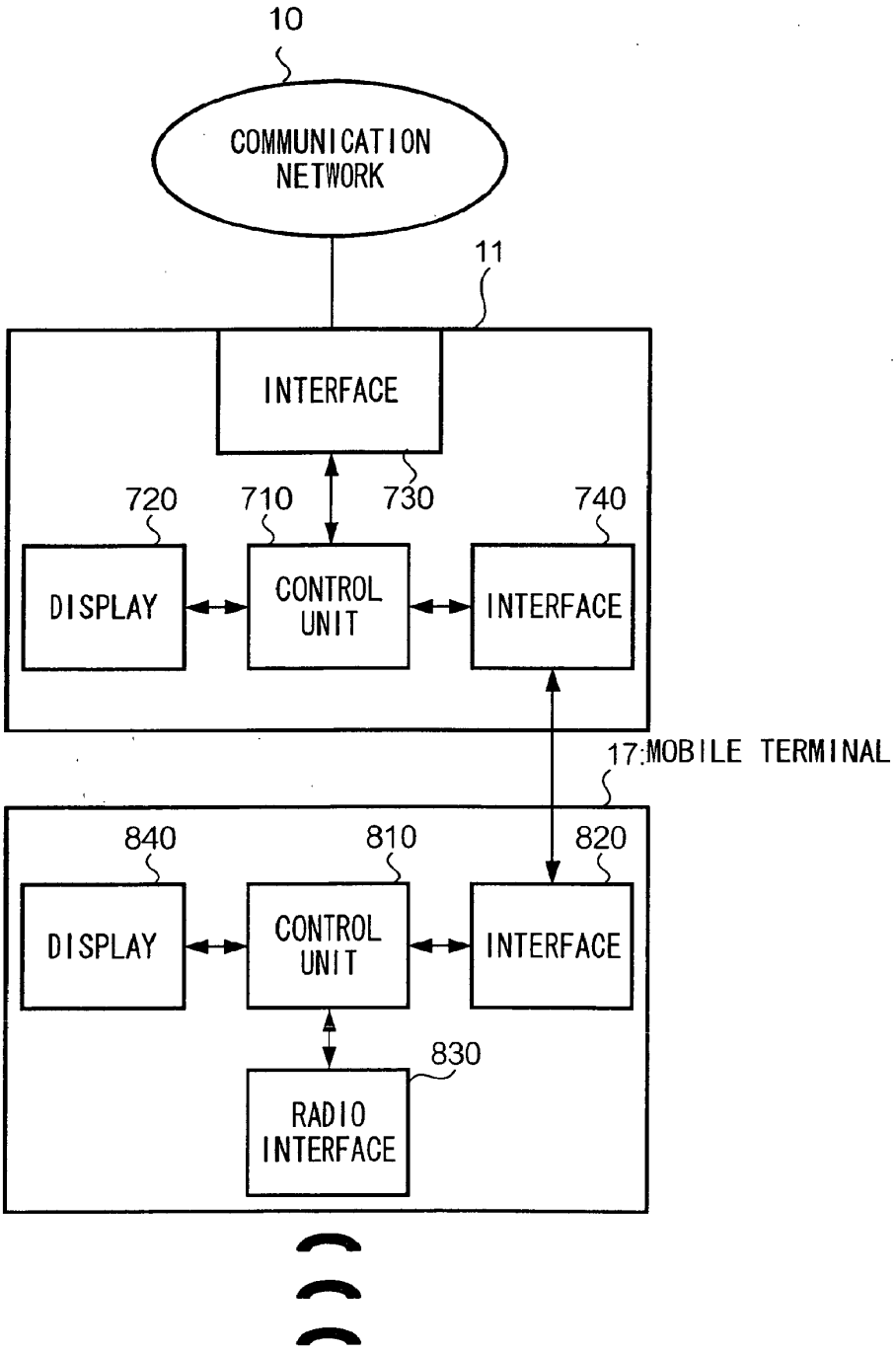


FIG. 4



APPL-1002
APPLE INC. / Page 404 of 1892

FIG. 5



APPL-1002
APPLE INC. / Page 405 of 1892

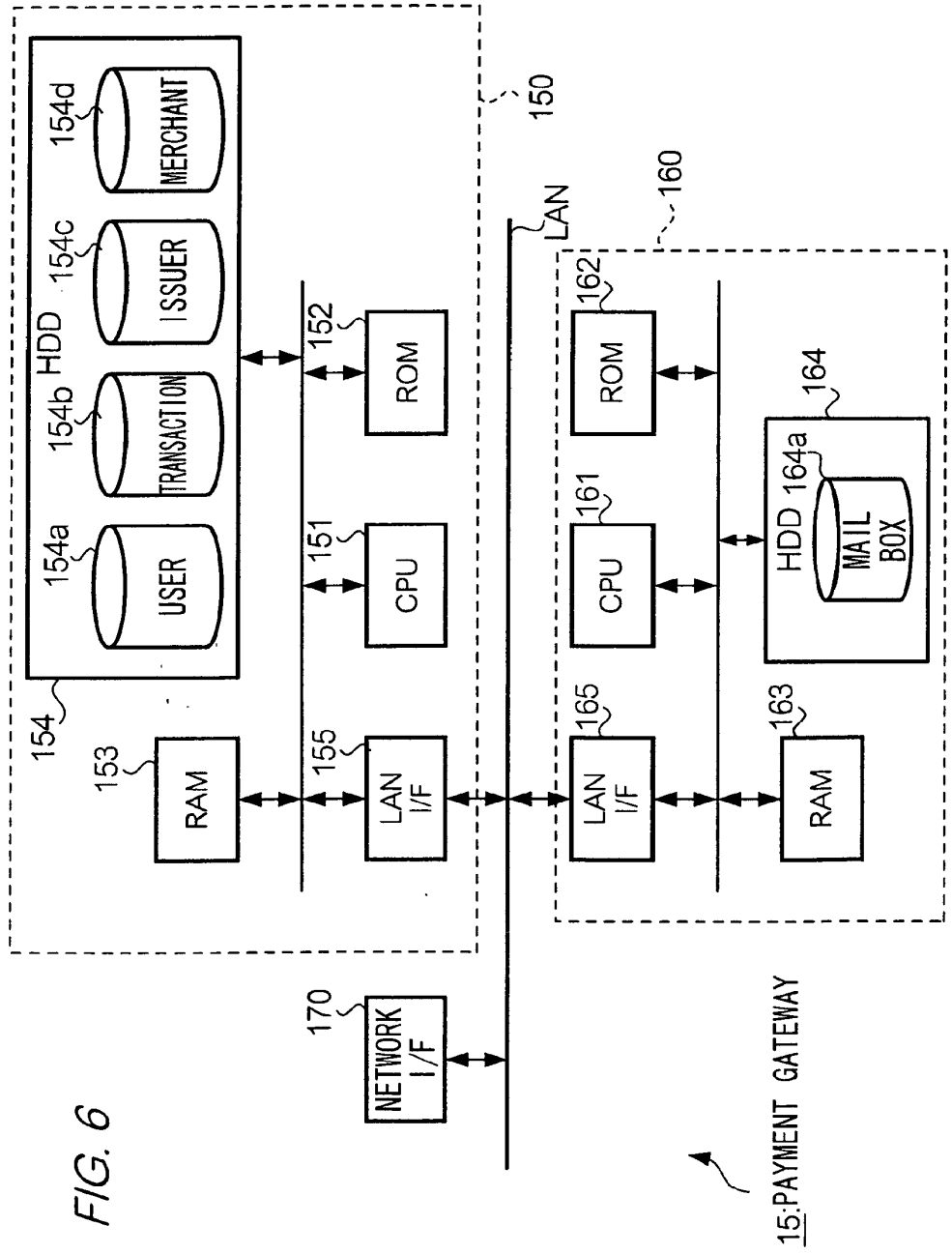
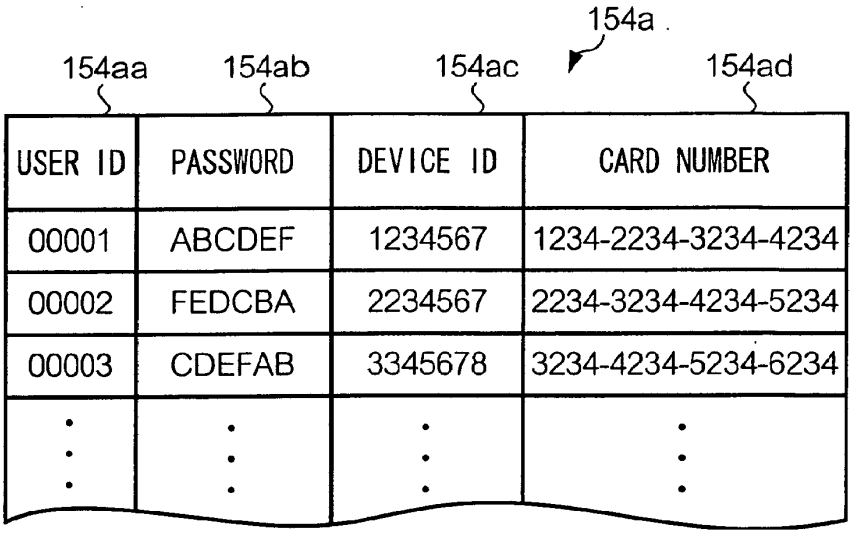


FIG. 6

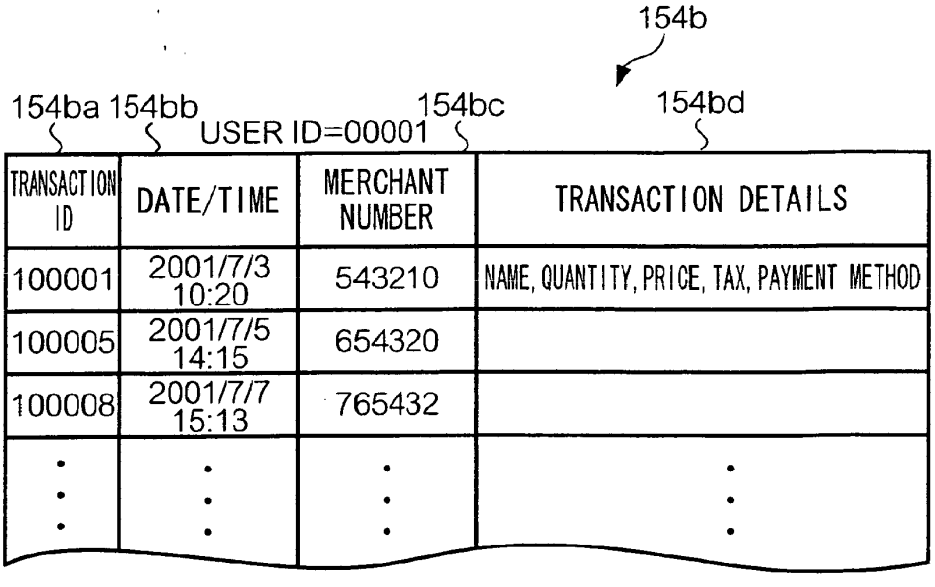
APPL-1002
APPLE INC. / Page 406 of 1892

FIG. 7



USER ID	PASSWORD	DEVICE ID	CARD NUMBER
00001	ABCDEF	1234567	1234-2234-3234-4234
00002	FEDCBA	2234567	2234-3234-4234-5234
00003	CDEFAB	3345678	3234-4234-5234-6234
⋮	⋮	⋮	⋮

FIG. 8



TRANSACTION ID	DATE/TIME	MERCHANT NUMBER	TRANSACTION DETAILS
100001	2001/7/3 10:20	543210	NAME, QUANTITY, PRICE, TAX, PAYMENT METHOD
100005	2001/7/5 14:15	654320	
100008	2001/7/7 15:13	765432	
⋮	⋮	⋮	⋮

APPL-1002
APPLE INC. / Page 407 of 1892

FIG. 9

154c

154ca 154cb 154cc

CARD NUMBER	ISSUER CODE	ISSUER NAME
1525000000～1525059999	2a11111	A
145259000～1452590000	2a22222	B
153996010～153996010	2s33333	C
13500～13560	2a11111	A
13600～13600	2s44444	D

FIG. 10

154d

154da 154db 154dc 154dd 154de

MERCHANT CODE	MERCHANT NAME	ISSUER NAME	ISSUER NAME	PAYMENT METHOD				
				L	I	B	PB	R
1111111111	A	2a11111	A	○	○	×	×	○
2222222222	B	2a22222	B	○	○	×	○	○
2222222222	B	2s44444	D	○	×	○	×	×
3333333333	C	2a22222	B	○	×	○	○	×
4444444444	D	2s33333	C	○	×	×	×	○

APPL-1002
APPLE INC. / Page 408 of 1892

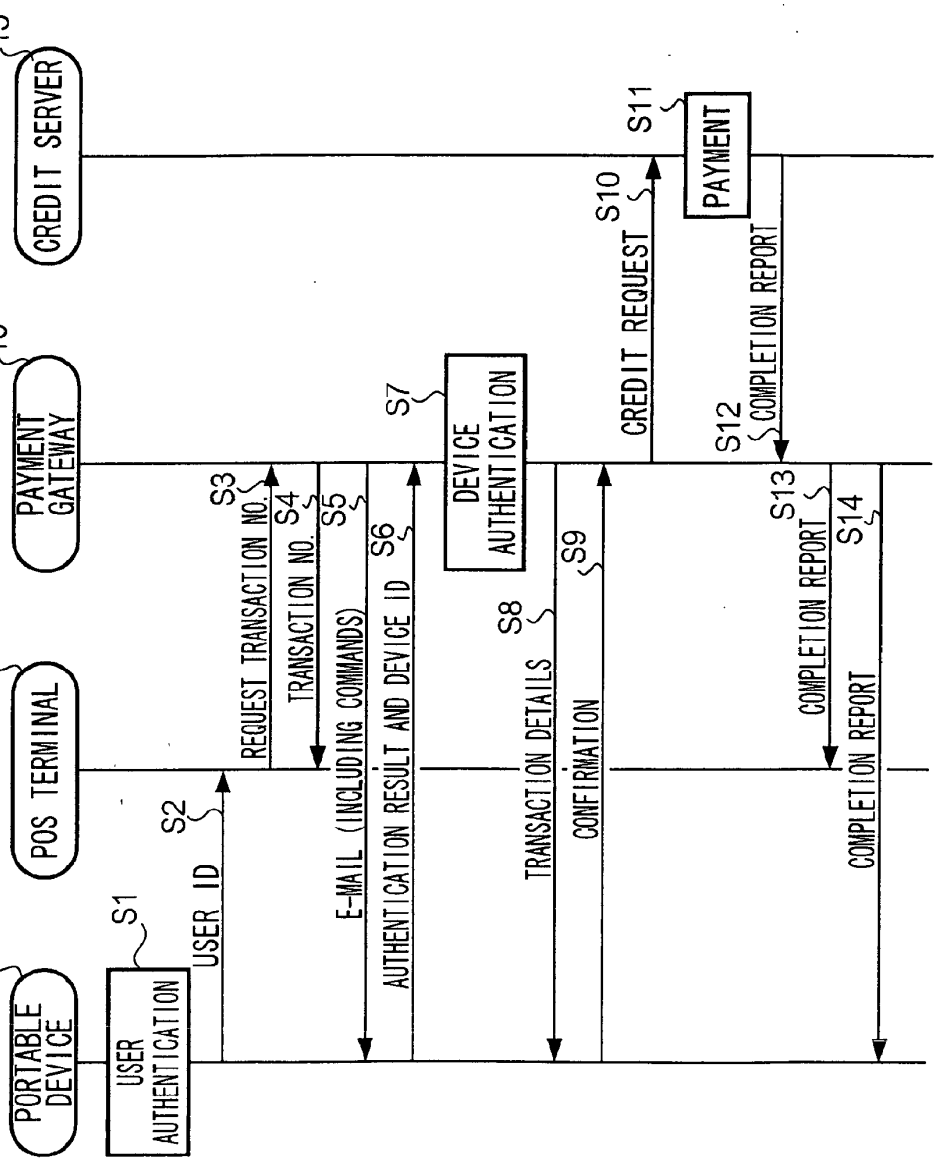
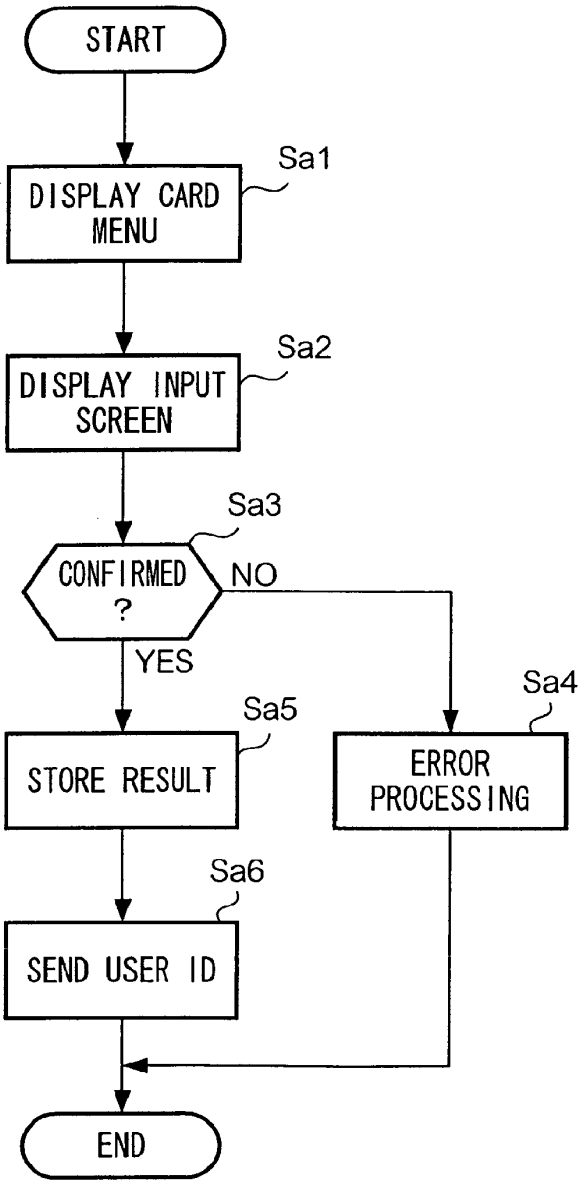


FIG. 11

APPL-1002
APPLE INC. / Page 409 of 1892

FIG. 12



APPL-1002
APPLE INC. / Page 410 of 1892

FIG. 13

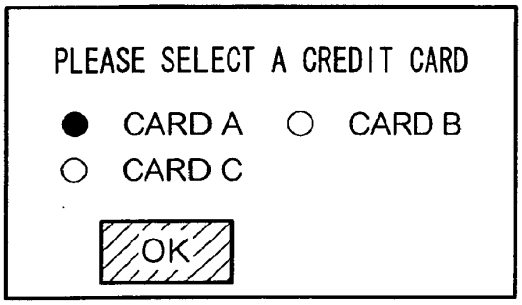
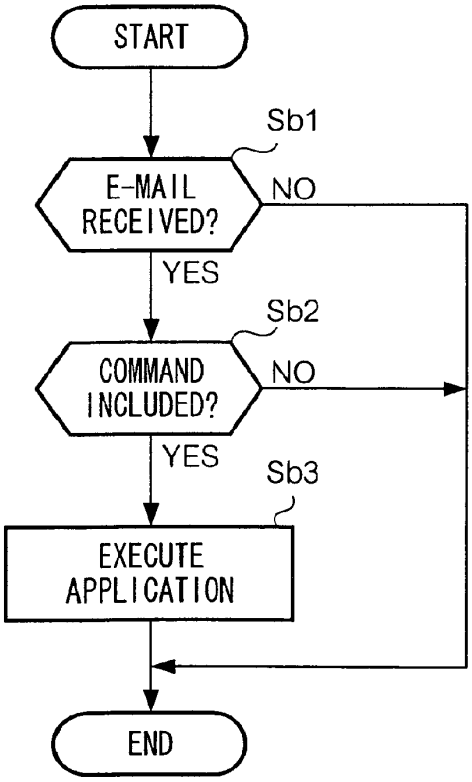
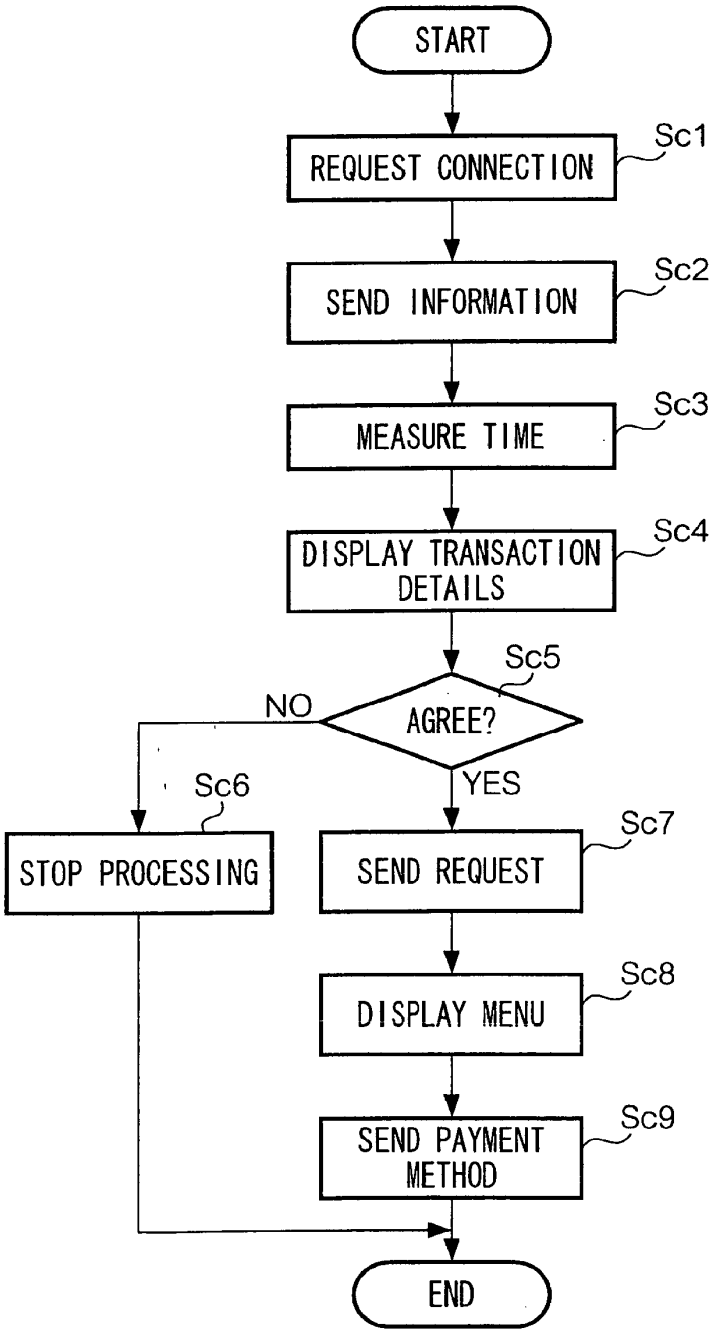


FIG. 14



APPL-1002
APPLE INC. / Page 411 of 1892

FIG. 15



APPL-1002
APPLE INC. / Page 412 of 1892

FIG. 16

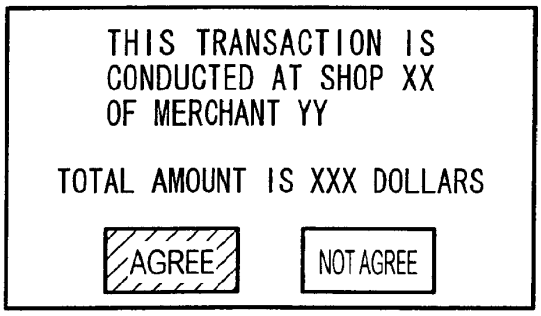
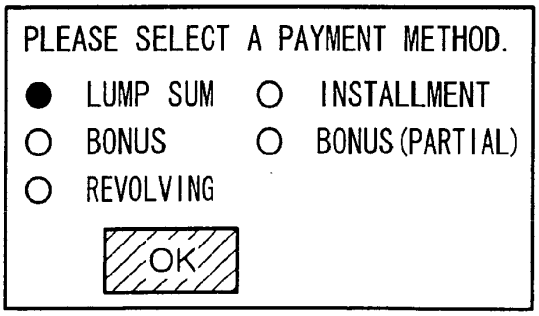
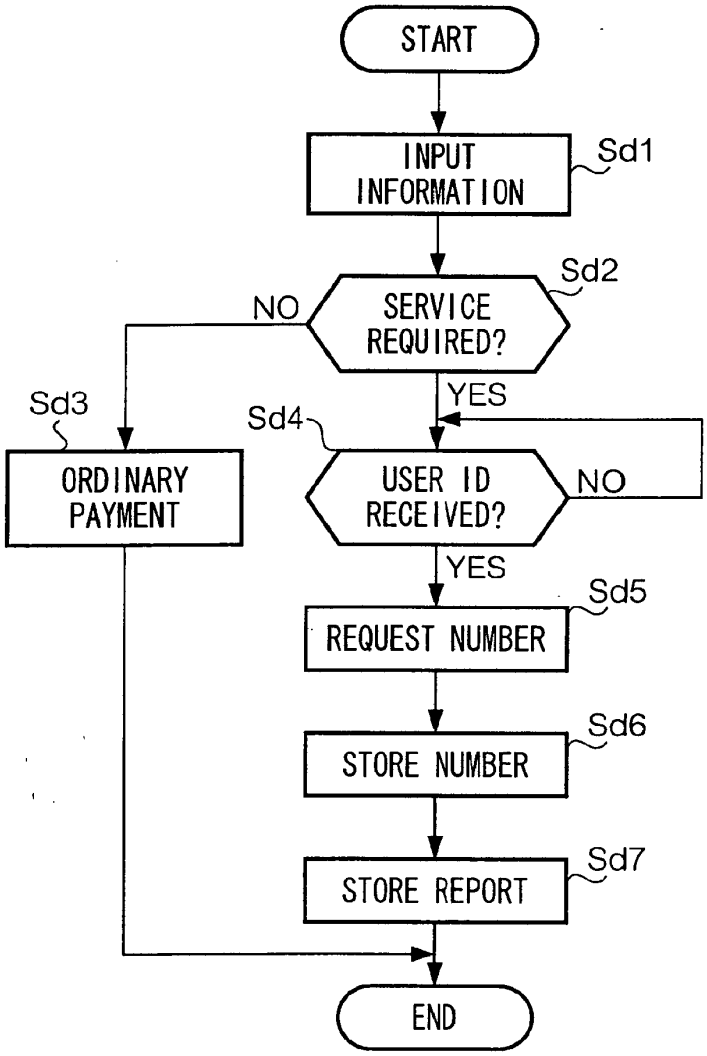


FIG. 17



APPL-1002
APPLE INC. / Page 413 of 1892

FIG. 18



APPL-1002
APPLE INC. / Page 414 of 1892

FIG. 19

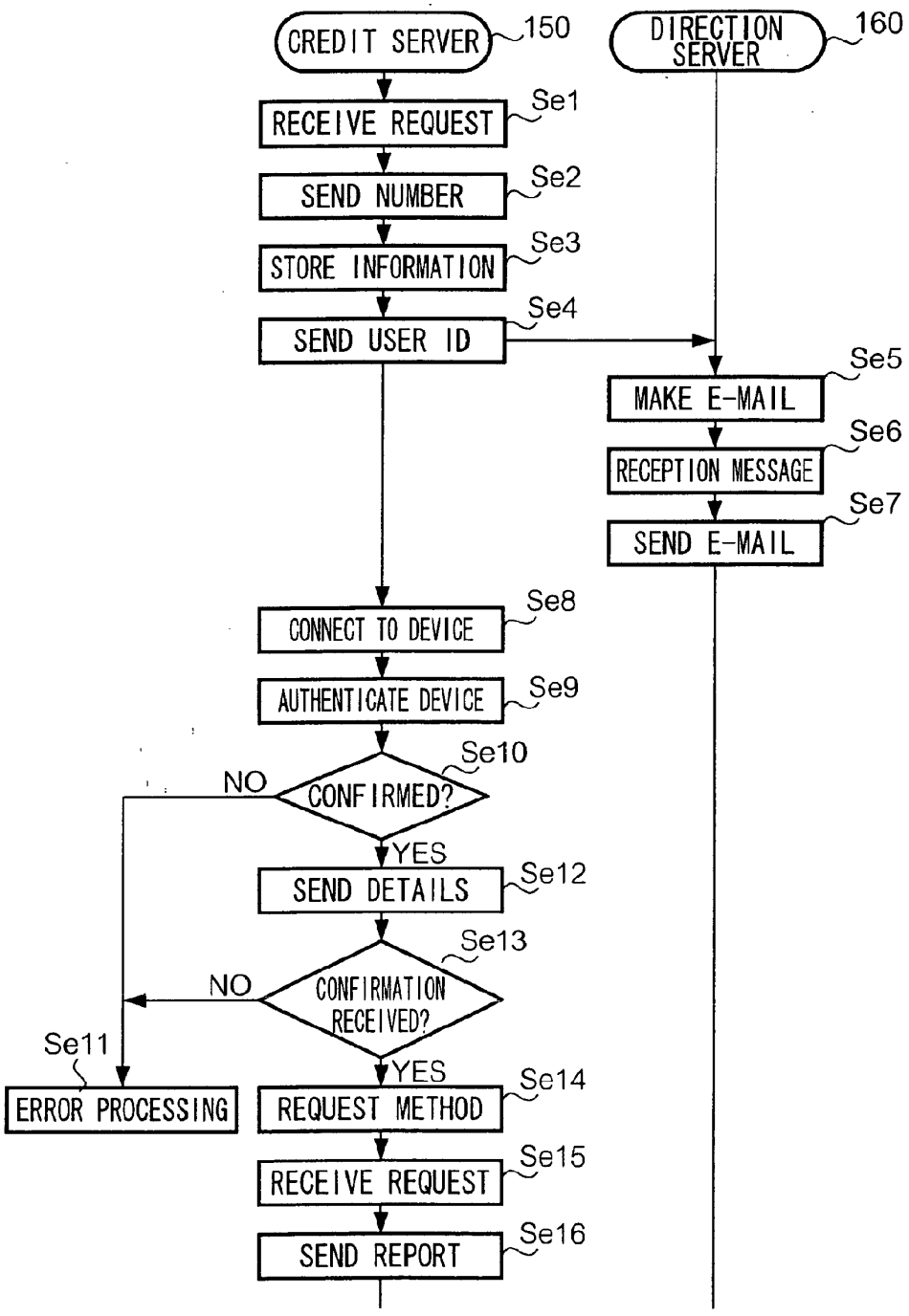
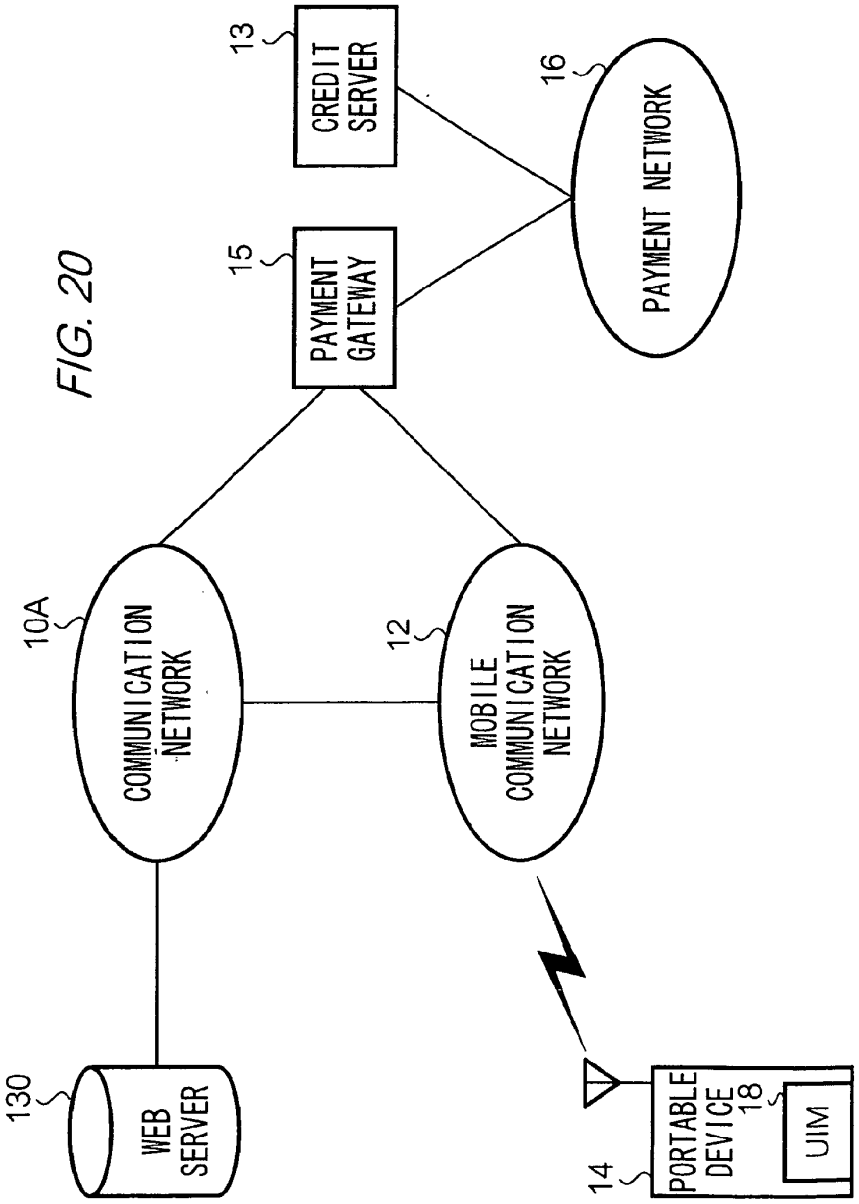
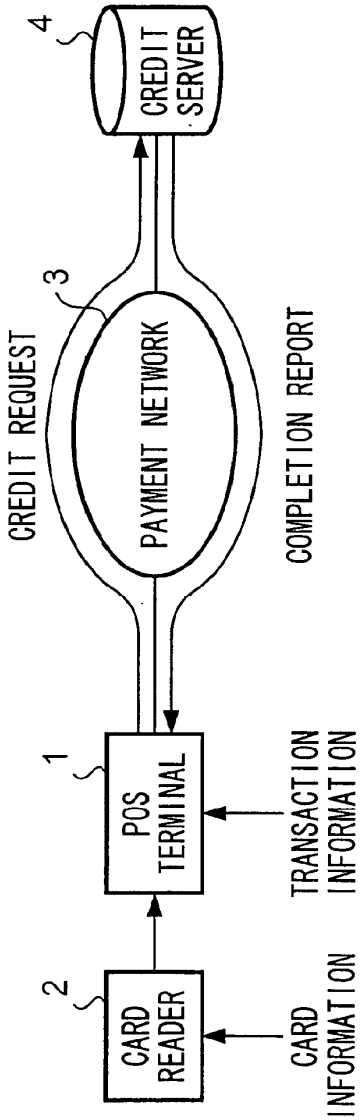

CREDIT SERVER
150
DIRECTION SERVER
160
RECEIVE REQUEST
Se1
SEND NUMBER
Se2
STORE INFORMATION
Se3
SEND USER ID
Se4
MAKE E-MAIL
Se5
RECEPTION MESSAGE
Se6
SEND E-MAIL
Se7
CONNECT TO DEVICE
Se8
AUTHENTICATE DEVICE
Se9
CONFIRMED?
Se10
NO
YES
SEND DETAILS
Se12
CONFIRMATION RECEIVED?
Se13
NO
YES
ERROR PROCESSING
Se11
REQUEST METHOD
Se14
RECEIVE REQUEST
Se15
SEND REPORT
Se16

FIG. 20



APPL-1002
APPLE INC. / Page 416 of 1892

FIG. 21



APPL-1002
APPLE INC. / Page 417 of 1892

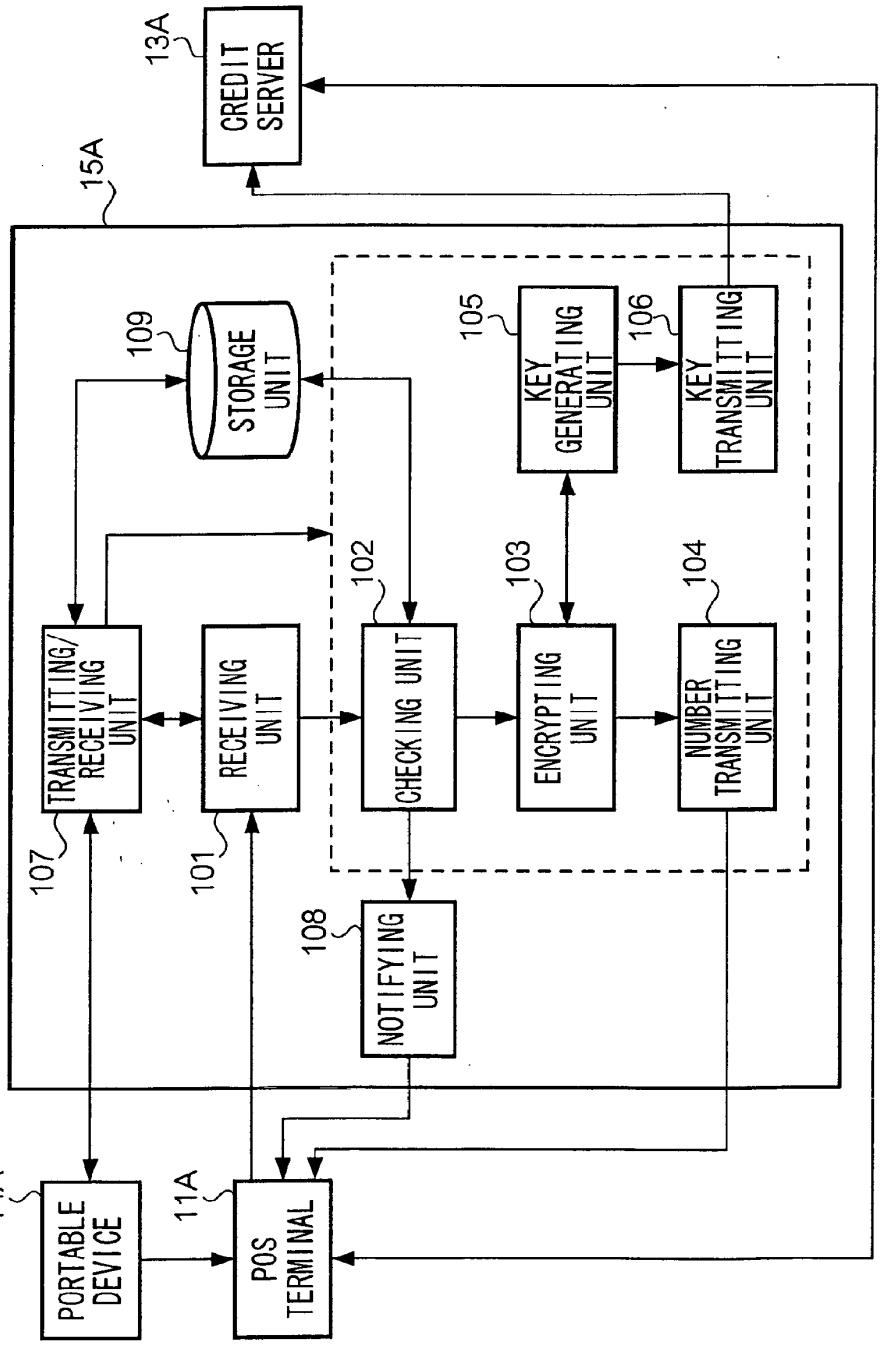

13A
CREDIT SERVER
15A
109
STORAGE UNIT
105
KEY GENERATING UNIT
106
KEY TRANSMITTING UNIT
102
103
104
TRANSMITTING/ RECEIVING UNIT
RECEIVING UNIT
CHECKING UNIT
ENCRYPTING UNIT
NUMBER TRANSMITTING UNIT
107
101
108
NOTIFYING UNIT
14A
11A
PORTABLE DEVICE
POS TERMINAL

FIG. 22

FIG. 23

ISSUER CODE	PAYMENT METHOD	MERCHANT CODE
.....	.....	.....
.....	.....	.....
.....	.....	.....
⋮	⋮	⋮

APPL-1002
APPLE INC. / Page 419 of 1892

FIG. 24A

MERCHANT CODE FOR CREDIT	PAYMENT METHOD	MERCHANT CODE
• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •
: :	: :	: :

FIG. 24B

USER NAME	ADDRESS	CARD NUMBER	EXPIRATION	LIMIT
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
: :	: :	: :	: :	: :

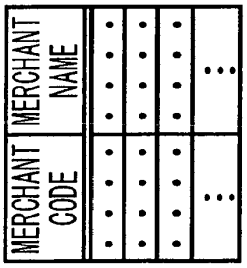
FIG. 24C

CARD NUMBER	KEY	TYPE	DATE	SERIAL NO.	MERCHANT NUMBER	AMOUNT NO.	PAYMENT METHOD	MERCHANDISE CODE
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
: :	: :	: :	: :	: :	: :	: :	: :	: :

FIG. 24D

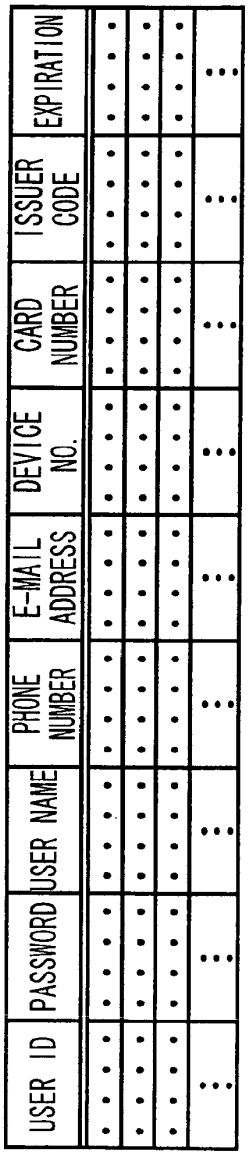
MERCHANT NUMBER	TYPE	DATE	SALES	CARD NUMBER	PAYMENT METHOD
• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
: :	: :	: :	: :	: :	: :

APPL-1002
APPLE INC. / Page 420 of 1892



MERCHANT CODE	MERCHANT NAME
• • • •	• • • •
• • • •	• • • •
• • • •	• • • •
: :	: :

FIG. 25A

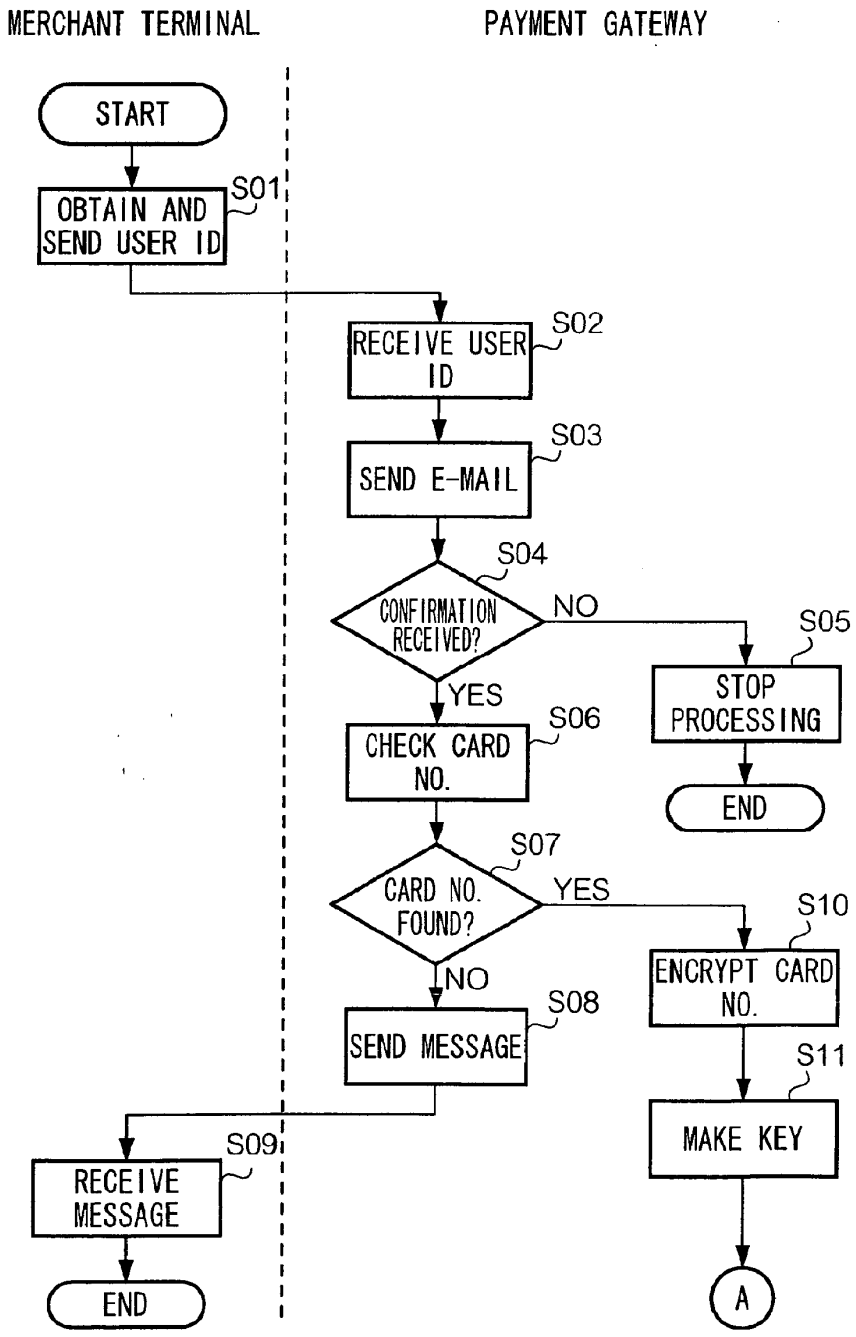


USER ID	PASSWORD	USER NAME	PHONE NUMBER	E-MAIL ADDRESS	DEVICE NO.	CARD NUMBER	ISSUER CODE	EXPIRATION
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
: :	: :	: :	: :	: :	: :	: :	: :	: :

FIG. 25B

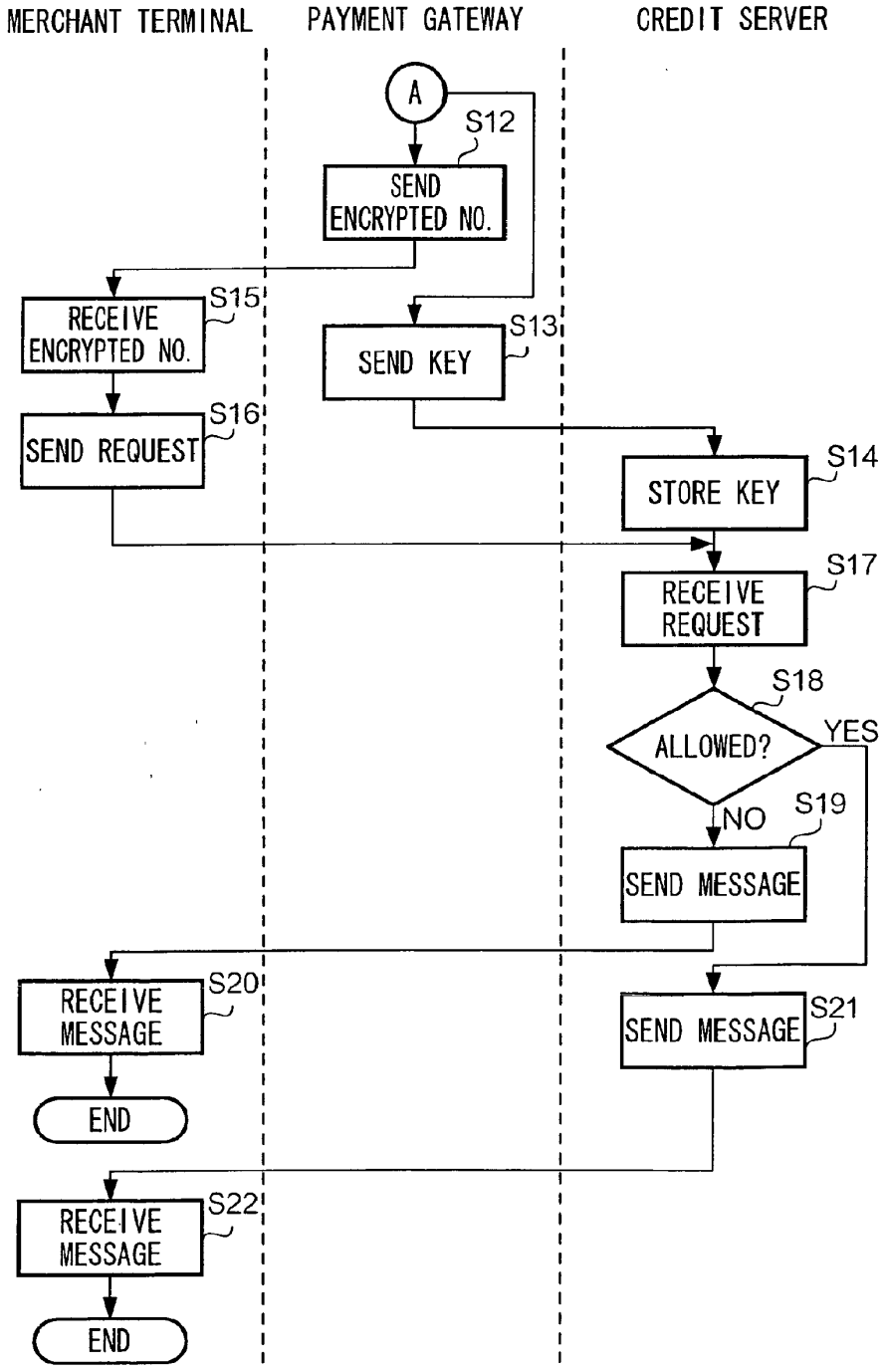
APPL-1002
APPLE INC. / Page 421 of 1892

FIG. 26



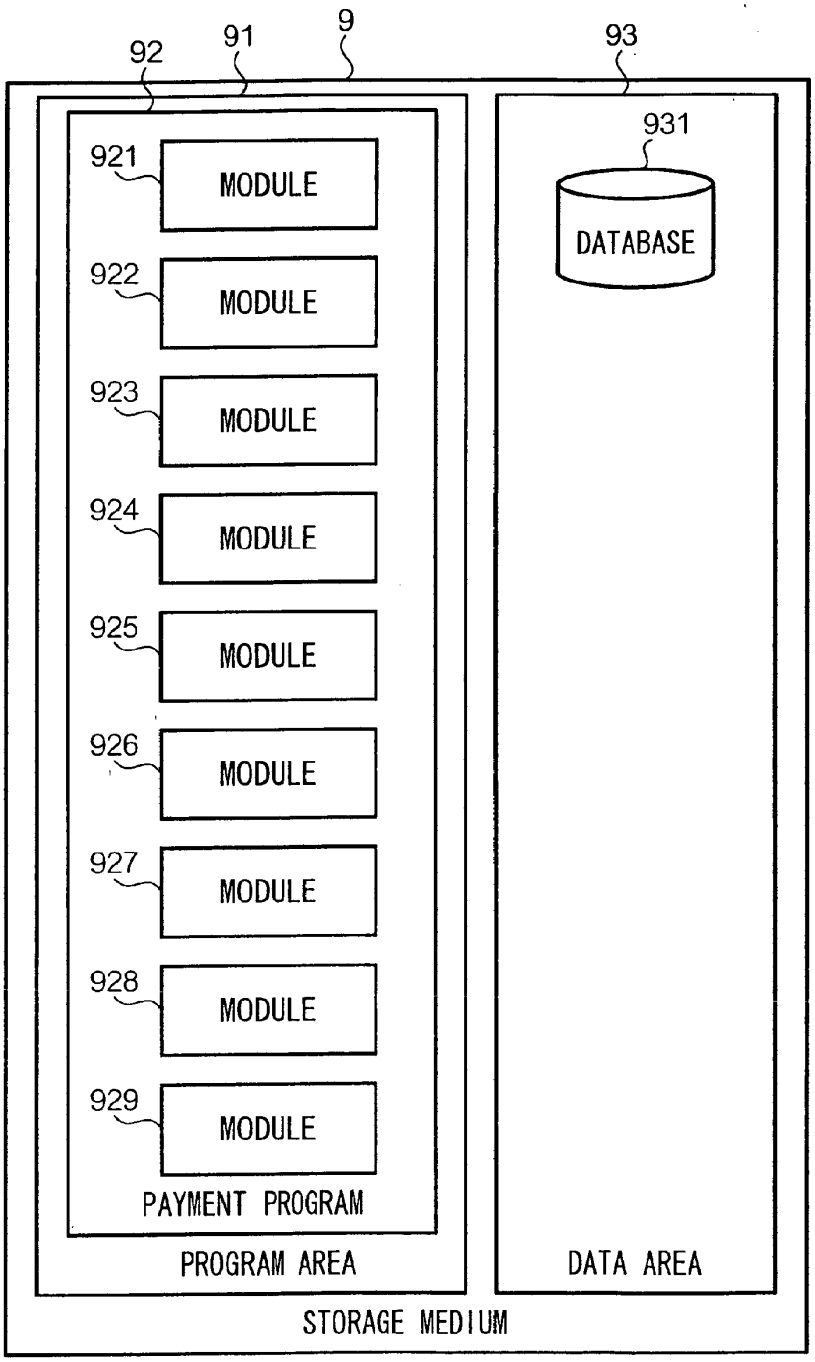
APPL-1002
APPLE INC. / Page 422 of 1892

FIG. 27



APPL-1002
APPLE INC. / Page 423 of 1892

FIG. 28



APPL-1002
APPLE INC. / Page 424 of 1892

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 084 921 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2008/046161 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2008/046161 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2008/046161 (art. 153(3) CBE).

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/046161 A1

(51) International Patent Classification:
H04Q 7/22 (2006.01) *H04M 3/493* (2006.01)

(21) International Application Number:
PCT/AU2007/001599

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905829 19 October 2006 (19.10.2006) AU

(71) Applicant *(for all designated States except US)*: **DELOITTE SERVICES PTY LTD** [AU/AU]; Level 1, 225 George Street, Sydney, NSW 2000 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **NGO, Duc, Anh** [—/AU]; 2/9 Fabian Court, Maribyrnong, VIC 3032 (AU).

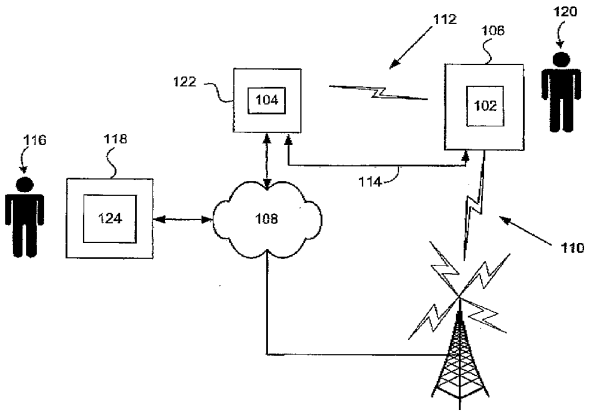
(74) Agent: **BLAKE DAWSON WALDRON PATENT SERVICES**; Level 35, Grosvenor Place, 225 George Street, Sydney, NSW 2000 (AU).

(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, ME, 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).

Published:
— *with international search report*

(54) Title: AN INTERACTIVE SYSTEM AND PROCESS



(57) Abstract: A method of delivering an instruction (206) to a mobile user device (106) connected to a network (110) is disclosed. The method comprising the steps of receiving an interactive workflow (202), translating the interactive workflow into the instruction (206) in a form executable by the mobile user device (106), and sending a message (208) including the instruction (206) to the mobile user device (106).

WO 2008/046161 A1

AN INTERACTIVE SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates generally to a method of delivering an instruction to a mobile user device connected to a network.

BACKGROUND

Amongst the wide variety of portable electronic devices available today, mobile phones have become particularly pervasive, with more than double the penetration of the Internet. These devices have rapidly advanced in capability and can do far more than Voice and SMS. Using these capabilities to deliver and execute applications that provide customisable interactivity to mobile phones and other devices is highly desirable but continues to be a challenging endeavour due the varied types of largely incompatible devices and platforms on the market.

Most interactive applications for mobile phones involve either Short Message Service (SMS) or the development of dedicated applications that address specific business requirements. SMS interactivity suffers from poor usability (the user has to be familiar with idiosyncratic commands) and security issues (SMS source addresses can be faked), thus limiting their usage to simple, non-sensitive transactions. Furthermore, an organisation wishing to use SMS to interact with its customers needs to come to some commercial arrangement with the telecommunications provider in order to establish billing procedures and so on. This can be inconvenient for the organisation, and may also be quite expensive, both to set up and also to operate on an on-going basis.

The dedicated applications are an attempt to address these shortcomings by developing programming code that is executed by the mobile device to perform a specific task. This involves significant amounts of time, at least because mobile phones from different manufacturers are not usually binary compatible and cannot execute the same executable applications. Additionally, these applications are limited to the functionality required at the time of development, and thus may not support additions or modifications to that functionality. As can be appreciated, distributing changes to these applications is similarly quite a tedious process, typically requiring the user to manually download and install an updated version of the application on their telephone.

SUMMARY OF THE INVENTION

According to one aspect of the invention there is provided a method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

According to another aspect of the invention there is provided a method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

According to yet another aspect of the invention there is provided computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

Preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language. More preferably the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

Preferably the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device. More preferably the

step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

Preferably the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

Preferably the step of translating the interactive workflow includes tailoring the instruction to the specification.

Preferably the step of translating the interactive workflow includes tailoring the instruction to a device operating system.

Preferably the step of sending the message includes the step of sending a unique message identifier. More preferably the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

Preferably the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network. More preferably the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS. Alternatively, the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

Preferably the method further comprises the step of the mobile user device receiving the set of instructions and the unique message identifier. More preferably the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

Preferably the method further comprises the step of receiving a response to the instruction from the mobile user device. More preferably the step of receiving a response includes the step of receiving a response identifier from the device. Even more preferably the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

Preferably the method includes the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow from the external or third party. More preferably the method includes the step of sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow from the external or third party.

Preferably the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface from the external or third party. More preferably the step of receiving a request for an Application Programming Interface is received from the external or third party. Even more preferably the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

Preferably the method also comprises the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

In accordance with the present invention, there is also provided an interactive process executed by a computer system or device, the process including:

receiving one or more SMS messages including instruction data representing one or more instructions for execution on said system or device to determine information;

executing said one or more instructions to determine said information; and

sending one or more SMS messages including response data representing said information.

Advantageously, said information may include system information determined from said system or device and/or user information determined from a user of said system or device.

Preferably, said execution causes generation of an interactive user interface on a display of said system or device, and the process includes receiving response data representing said information from a user of said system or device in response to said interactive display.

Preferably, said one or more instructions are executed by a virtual machine of said system or device.

The present invention also provides an application component for a system or device, the applicationcomponent including:

a message receiver for processing one or more received SMS messages to generate one or more instructions for execution on said device to determine information;

an execution component for executing said one or more instructions of said application data to determine said information; and

a message sender for generating one or more SMS messages including response data representing said information.

Preferably, the application component further includes a data management component for storing sets of instructions on non-volatile storage means and for retrieving a selected one of the stored sets of instructions for execution.

Preferably, said execution component is adapted to generate an interactive display for a user of said system or device, and to receive response data representing said information from a user of said system or device in response to said interactive display.

The present invention also provides an interactive process for execution by a system or device, including:

receiving message data including header data and encrypted payload data;

selecting one of a plurality of encryption keys on the basis of said header data; and

decrypting said payload data using the selected encryption key.

Preferably, said header data includes index data representing an index for said plurality of encryption keys.

Advantageously, said payload data may represent one or more instructions for execution on said system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions on a remote system or device.

The present invention also provides an interactive process for execution by a system or device, including:

generating payload data for sending to a remote system or device;

selecting one of a plurality of encryption keys;

encrypting said payload data using the selected encryption key;

generating message data for sending to said remote system or device, said message data including header data and the encrypted payload data, wherein said header data includes data representing an index for said plurality of encryption keys to allow said remote system or device to determine the selected encryption key and thereby to decrypt said payload data.

Advantageously, said payload data may represent one or more instructions for execution on said remote system or device to determine information.

Advantageously, said payload data may represent information in response to execution of one or more instructions.

Preferably, the process includes generating said plurality of encryption keys and sending said plurality of encryption keys to said remote system or device.

Preferably, the process includes associating said plurality of encryption keys with an identifier of said remote system or device.

The present invention also provides an interactive process, including:

receiving programming instructions for generating an interactive display on a remote system or device;

compiling said programming instructions to generate compiled instruction data;

sending said compiled instruction data to said remote system or device to generate an interactive display on said second remote system or device;

receiving response data representing at least one user response to said interactive display; and

sending response data representing said at least one user response.

The present invention also provides an interactive process, including:

receiving workflow instructions from a plurality of entities;

processing said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

sending said interactive applications to said user devices for execution.

Preferably, said interactive applications are sent to said user devices using short message service (SMS).

Preferably, said user devices include mobile telephones.

The present invention also provides an interactive system for managing interaction with users of remote systems and/or devices, the interactive system being adapted to:

receive workflow instructions from a plurality of entities;

process said workflow instructions to generate interactive applications for execution on a plurality of user devices; and

send said interactive applications to said user devices for execution.

The present invention also provides a system having components for executing any one of the above processes.

The present invention also provides a computer-readable storage medium having stored thereon program instructions for executing any one of the above processes.

The present invention also provides an interactive system, including:

a gateway component for processing received workflow data to generate instructions for generating an interactive display on a user device, the gateway component being adapted to send said instructions to said user device for execution; and

an execution component of said user device to receive and execute said instructions to generate said interactive display, to receive response data representing at least one response of said user to said interactive display; and to send said response data to said gateway component.

Preferably, said user device is a mobile telephone.

Advantageously, the instructions may be sent to said gateway component in one or more SMS messages.

Advantageously, said user response data may be sent to said user device in one or more SMS messages.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an interactive system;

Figure 2 is a schematic diagram of the high level process and data flow of an interactive process of the interactive system;

Figure 3 is a block diagram of a mobile telephone on which a client application of the interactive system is installed;

Figure 4 is a block diagram of the client application of the interactive system;

Figure 5 is a flow diagram of the life cycle of an interactive application generated by the interactive process and system;

Figure 6 is a block diagram of an application gateway of the interactive system;

Figure 7 is a block diagram of a computer system on which the application gateway is installed;

Figure 8 is a schematic diagram of the process and data flow of an opt-in process of the interactive system;

Figure 9 is a schematic diagram illustrating the use of encryption key sets to establish an encrypted communications channel between the client application and the application gateway;

Figure 10 is a schematic diagram of the process and data flow involved in conducting secure communications between the client application and the application gateway;

Figure 11 is a schematic diagram illustrating the default behaviour of the interactive system and process whereby a particular application gateway transmits instructions to a particular client application, and the resulting response data is returned to the same application gateway that sent the instructions;

Figure 12 is a schematic diagram similar to that of Figure 11, but illustrating the redirection of response data to a different application gateway from the application gateway that sent the corresponding instructions;

Figure 13 is a schematic diagram illustrating the structure of messages exchanged between the application gateway and the client application;

Figure 14 is a schematic diagram illustrating the structure of payload data of the messages shown in Figure 13;

Figure 15 is a schematic diagram illustrating the structure of each data part of the payload data of Figure 14;

Figure 16 is a schematic diagram illustrating the fifteen different types of instructions supported by the interactive system and process;

Figure 17 is a schematic diagram illustrating the structure of an SMS message generated by the interactive system and process;

Figure 18 is a schematic diagram illustrating how the interactive system uses multiple SMS messages to transmit instructions constituting an application whose length is greater than 133 bytes;

Figure 19 is a flow diagram of an SMS transmission process of the system;

Figure 20 is a flow diagram of an SMS receiving process of the system;

Figure 21 is a flow diagram of an application execution process executed by the execution engine of the system;

Figure 22 is a schematic diagram illustrating the structure of response data sent from the client application to the application gateway;

Figure 23 is a schematic diagram illustrating how the system uses parameter names provided in instructions to label corresponding responses;

Figure 24 is a schematic diagram illustrating execution branching in the client application;

Figure 25 is a schematic diagram illustrating the use of branch domains to label responses having the same parameter name;

Figure 26 is a schematic diagram illustrating the use of a branch name stack to determine control flow;

Figure 27 is a schematic diagram illustrating the user interface components resulting from selecting different branches of an interactive application;

Figure 28 is a schematic diagram illustrating the inclusion of a 'back' button on each user interface display;

Figure 29 is a schematic diagram illustrating the use of an executed instruction stack to implement the 'back' button of Figure 28;

Figure 30 is a screen shot of a user interface of the application gateway for entering scripting language instructions and for submitting those instructions to an instruction compiler of the application gateway;

Figure 31 is a source code listing of a function illustrating how the system APIs can be used to send details of a booking to a mobile telephone for display to a user, and to receive the user's response indicating whether they user accepts or rejects the booking;

Figure 32 is a partial listing of a scripting language application, illustrating the use of control flow branches in the scripting language;

Figure 33 is a schematic diagram illustrating the user interface components generated from the scripting language example of Figure 32;

Figure 34 is a schematic diagram illustrating the use of nested user interface displays generated by the system;

Figures 35 and 36 are schematic diagrams illustrating the appearance and structure of general user interface displays generated by the system;

Figure 37 is a schematic illustration of a slider control display generated by the system;

Figure 38 is a schematic diagram illustrating the use of single and multiple selections in user interface displays generated by the system; and

Figure 39 is a schematic diagram illustrating how the branch names of nested menus are used to label parameter data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As shown in Figure 1, an interactive system includes at least one client application 102 and at least one application gateway 104. Each client application 102 is a component of a corresponding user device 106 that can communicate with the at least one application gateway 104 via one or more of a variety of communications means supported by the device 106, preferably including a combination of (i) an IP-based communications network 108 such as the Internet, (ii) a wireless wide-area communications network such as the global system for mobiles (GSM) telephone network, (iii) a local wireless network or link between the device 106 and the at least one application gateway 104, such as an infra-red link, Wi-Fi or Bluetooth network 112, and/or (v) a direct cable connection 114

using a standard communications protocol such as RS-232, universal serial bus (USB), or FireWire (IEEE 1394). The interactive system allows an application developer 116 using a standard computer system 118 to rapidly develop and deploy an interactive workflow or application for execution on one or more user devices 106 in order to interact with the users 120 of those devices 106, and to receive response data representing at least one response of each user 120 to the interactive application.

The interactive workflow or application includes a set of instructions for presenting information to a user 120 of each mobile device 106 in an interactive display or user interface, and for retrieving each user's response(s) to that information. Typically, the information presented to a user 120 will include one or more questions displayed on a display screen of the user's device 106 (and possibly also audio played on a sound transducer of the device 106), and each of the user's responses is provided by the user interacting with one or more user-interface (UI) components or input controls of the interactive display. Each response can be in the form of freeform text typed into a textbox, or the result of the user interacting with another type of input control, such as radio buttons, check boxes, sliders, simple menus, nested menus, and so on. To some extent, these possibilities are determined by the capabilities of the device 106. However, because the workflow supported by the system also includes control flow features similar to those provided by high-level programming languages, the workflow instructions generated by the system are also considered to constitute an interactive software application that is executed on the user device 106.

In the described embodiment, the user device 106 is a mobile telephone, but alternatively could be some other type of portable or handheld device such as a personal data assistant (PDA), and hence is also referred to hereinafter as "the mobile device 106". However, even though the device 106 is described as being "mobile" or "portable", it will be appreciated by those skilled in the art that the systems and processes described herein could alternatively be used in conjunction with other types of devices and systems that need not even be portable. For example, the client application 102 could even be installed on a standard personal computer system (rather than the portable device 106) in order to rapidly develop and deliver interactive applications to a standard personal computer, for example.

In the described embodiment, the client application 102 is a software application that is stored on the mobile device 106, either as part of the device manufacturing or configuration prior to sale, or subsequently deployed as required via GPRS, Bluetooth, Infrared or a phone specific channel (*e.g.*, a data cable), allowing it to be installed on a wide variety of different types of device. However, it will be apparent to those skilled in the art that the client application 102 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

Similarly, the application gateway 104 is a software application that is installed on and executed by a standard computer system 122, such an Intel™ IA-32 computer server executing a Windows™ operating system. The computer system 122 includes standard hardware components 702, and software components 704. The hardware components 702 include at least one processor 706, a communications interface (*e.g.*, network interface card) 708, random access memory 710, non-volatile (*e.g.*, hard disk storage) 712, user input device (*e.g.*, keyboard, mouse or other pointing device) 714, and a display adapter and device 716, all interconnected by a system bus 720. The software components 704 include the application gateway 104, and a standard operating system 718 such as Microsoft Windows. Additionally, a third party application 124, shown as being installed on the developer's computer 118, may additionally or alternatively be installed on the same computer system 122 on which the application gateway itself is located 104, as shown. However, although the application gateway 104 is described as being a software application, it will be apparent to those skilled in the art that the application gateway 104 and its processes could alternatively be implemented either in part or in total by one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), for example.

The client application 102:

(i) verifies a set of instructions sent by the application gateway 104;

(ii) interprets these instructions;

(iii) interacts with the user device 106 and/or the user 120 in accordance with the set of instructions; and

(iv) sends responses back to the gateway 104 or other computer system or device.

The application gateway 104 is effectively a backend component that:

(i) maintains a database of user devices of the interactive system (*i.e.*, devices on which the client application 102 has been installed);

(ii) generates and delivers interactive applications to the mobile device 106 via any one of a wide range of communication channels;

(iii) ensures the integrity and authenticity of outgoing and inbound messages to and from the mobile device 106; and

(iv) provides application programming interfaces (APIs) to allow third-party applications 124 to deploy an interactive application to the mobile device 106 and to receive corresponding responses generated by the client application 102 on the mobile device 106.

Figure 2 is a schematic diagram illustrating the high level operation of the interactive process of the system in relation to the various components shown in Figure 1. At step 202, an external or third-party application 204 executing on the developer's computer system 118 (or, alternatively, on the gateway computer system 122) calls an API 616 of the application gateway 104 to describe the workflow that the developers of the device 106 want to deploy. In general, the workflow includes the steps of displaying information to a user, and then retrieving at least one response to that information. For example, a typical workflow might be to display a message on the mobile device 106, ask the user to enter their age, then display another message, and send the age back to the developer. These steps or instructions constitute an interactive application for execution on the mobile device 106.

The workflow defines:

(i) one or more addresses of respective user devices 106;

(ii) the steps to be performed on the one or more user devices 106;

(iii) the address of an alternate gateway server (if any) 104 to which responses are to be sent; if no address is given, then the responses will be sent to the same gateway server 104 that sent the application instructions;

(iv) how the response data returned to the application gateway should be processed (*e.g.*, returned to the developer's application 124, sent to the developer 116 by email, stored in a file, etc.); and

(v) the communication method(s) that are to be used to send the instructions to the user device 106 and to receive the corresponding response data.

At step 206, the application gateway 104 transforms the workflow described by the developer into a compressed, encoded, and encrypted format for transmission to the mobile device 106. The application gateway 104 also inserts a unique identifier or ID into the message and stores data associating that ID with the destination (*e.g.*, phone number, or network address) to which the workflow is to be sent.

The application gateway 104 transforms the message so that it can be transmitted via the appropriate communication means. For example, if the message is to be transmitted via SMS, the application gateway 106 splits a large message into smaller messages to comply with the GSM standard. All this is hidden from the developer. At step 208, the application gateway 104 then transmits the message to the device 106 specified by the developer.

At step 210, the client application 102 receives, un-compresses and decrypts the message(s), thereby verifying their integrity. If valid, at step 212 the client application 102 interrupts the user and requests that they complete the workflow. With the user's cooperation, the client application 102 interprets each instruction and performs a corresponding operation *e.g.*, display a message, collect the user's age, etc. that in most cases involves interacting with the user of the device 106.

At the end of the workflow, the client application 102 sends back to the application gateway 104 all the collected response data via the response channel specified in the workflow instructions by the application gateway 104. For example, if the response is to be returned via SMS, a response SMS is sent back to a phone number provided in the initial message(s). The client application 102 also encrypts the response message(s) and includes the unique message ID to ensure authenticity of the response.

When the application gateway 104 receives the response message at step 216, it decrypts the message and determines whether the ID of the message is valid for the phone number it was received from, using the destination and ID association stored previously. If the message is valid, then it is processed as specified by the developer *e.g.*, passes it on to a third-party application, emails the developer, stores it in a file, etc.

In addition to the above, the interactive system also provides capabilities for (i) storing (and subsequently updating) a set of instructions as a permanent or semi-permanent application stored on non-volatile storage of the user device 106 for execution at any time; *i.e.*, the application persists on the user's device; (ii) the distribution of encryption keys; and (iii) opt-in mechanisms to ensure that the mobile device 106 is not sent unsolicited applications, *e.g.*, if the application gateway 104 is shared by multiple vendors.

The interactive system and the interactive process executed by the interactive system are described in detail below.

As shown in Figure 3, the mobile device 106 is a standard mobile phone including hardware components 302 and software components 304. The hardware components 302 include a processor 306, read-only memory 308, random-access memory 310, flash memory 312, user interface components including user input components 314 (*e.g.*, microphone, keyboard, and, in some devices, touch-screen), output components 316 (*e.g.*, display screen, speaker), and one or more communications interfaces 318 allowing the device 106 to communicate with a mobile phone network 110, and, in some devices, also Bluetooth and/or Wi-Fi local wireless networks or an infrared link 112. In the preferred case of the mobile device 106 being a telephone, the device 106 also includes a SIM card 320. The software components include an operating system 322 such as the closed, proprietary operating systems installed on mobile telephones sold under brands such as Nokia and Motorola, Java platform Micro-edition (Java ME) 324, and the client application 102. However, if the operating system 322 is a more sophisticated operating system such as Symbian, Linux, Microsoft SmartPhone, PocketPC, Windows CE, or Windows Mobile, that provides sufficiently powerful application programming interfaces (APIs), then the J2ME component 324 can be omitted. As shown in Figure 4, the client application 102 includes a message sender component 402, a message receiver component 404, user interface (UI) widgets 406, a workflow execution engine 408, instant data storage 410, and permanent data storage 412. The client application 102 is a native application that is executed by the mobile device 106. The client application 102 can be installed by any one of a number of means, including WAP push, IP data packets (GPRS or 3G networks), Bluetooth, Infrared, or a phone-specific channel such as a data cable. The

client application 102 can be provided as a preinstalled application on the mobile phone 106 when purchased.

The message sender 608 sends response messages to the application gateway 104 in a format understood by the application gateway 104. It encrypts the message and includes ID provided with the initial application to confirm its authenticity.

The message receiver 606 decrypts and uncompresses instruction sets received from the application gateway 104. It implements message reception via a number of channels, including Bluetooth, Infrared, IP networks (GPRS or 3G), and SMS. The message receiver 606 also invokes the workflow execution engine 408 to process the instruction set.

The UI Widgets 406 are pre-built user interface components that instructions sent by the application gateway 104 can use to interact with the user.

The workflow execution engine 408 is responsible for running and maintaining state for the instructions currently being processed. It associates instructions with UI widgets as well as storing input from the device 106 and its user. It is also responsible for invoking the message sender 402 once the workflow is completed to initiate sending the response to the application gateway 104. The workflow execution can also be invoked by a timer if an instruction asks to be run at a specific time.

The client application 102 can simultaneously receive multiple workflow applications at any one time, and the instant data store 410 is effectively a first-in, first-out queue that stores these applications and processes them one by one until the instant data store 410 is empty.

The interactive system has the ability to make a sequence of instructions persistent on the mobile device 106 as an application. These sequences are identified by a unique label and are stored in the permanent data store 412, being in this embodiment the non-volatile flash memory 312. The application gateway 104 can issue commands to update or delete applications in the permanent data store 412.

Figure 5 is a flow diagram illustrating the life cycle of an execution instance of the client application 102 following receipt of an instruction from an application gateway 104. However, the client application 102 can be invoked at step 502 by either a new data event or a timer event. A new data event occurs when the client application 102 is activated by the mobile device 106 when new payload data addressed to the client application 102 is received. Timer events are set by a specific instruction that suspends execution of the instruction to a later date/time. The workflow engine 408 is responsible for scheduling the client application 102 to start and process the instruction set at that date/time.

Once invoked, at step 504 the instruction sequence is retrieved either reading data from the instant data store 410, in the case of a Timer event, or from the input channel in the case of a new data event. If the instruction data is retrieved from the input channel and is encrypted, at step 506 the client application 102 decrypts and verifies it as described below. If the data is valid, the workflow execution begins at step 508.

The workflow execution 508 processes the instructions step by step. This may or may not involve user interactions (as some instructions described in the Appendix can be handled without user interaction). Upon execution of a timer instruction specifying that execution should be postponed to a later time, further execution of instructions of the workflow application is suspended and the instruction set is stored placed in the instant data store 410 pending resumption at the specified time.

Once the workflow execution 508 is complete, the workflow application is removed from the instant data store 410. If the application is marked as persistent, the instruction set is saved to the permanent data store 412. The user can then invoke the instruction set at any time.

At step 510, the information collected by the workflow execution 508 is sent back to the application gateway 104 as response data. The client application 102 encrypts the response data in addition to including the unique message ID that verifies the authenticity of the response data.

As shown in Figure 6, the application gateway 104 includes an instruction compiler 602, a key manager 604, a message receiver 606, a message sender 608, an opt-in manager 610, persistent storage 612, and an application programming interface (API) 616.

The instruction compiler 602 translates workflow descriptions received from the developer 116 into a format that is optimized for delivery to and execution by the client application 102. The workflow description is written in a scripting language that is compiled by the instruction compiler 602. The developer can enter the workflow description directly into a text box and submit its contents to the compiler 602. This is typically used to rapidly prototype the look and feel of a workflow application. Alternatively, the workflow description can be submitted by making an API call to the compiler 602 from a high-level programming language such as C#, Java, or TCL, thus providing end-to-end application integration.

The message sender 608 encrypts the workflow instruction set. The encryption relies on requesting the key manager 604 to provide a random index and an encryption key that is specific to a particular user device 106 on which the instructions are to be executed. The index is sent in cleartext to the client application 102, which uses the index to look up the appropriate encryption key to decipher the message. The message sender 608 also generates a unique random identifier for the workflow application. The random identifier is a combination of a random identifier and an identifier of the party who sent the workflow description.

The message sender 608 uses the transport adapter 614 to deliver the actual message(s) containing the workflow application. The message sender 608 first checks with the Opt-in manager 610 to ensure that the client application 102 does not receive unsolicited applications which it has not opted into, as described below.

The transport adapter 614 abstracts the various methods of delivering an instruction set to the client application 102 on the mobile device 106. It uses device capability information stored in the persistent storage 612 to determine the capabilities of the device 106 and hence the best communication channel to deliver the message(s).

The transport adapter 614 provides plug-in support for new channel types dynamically by providing a set of messaging APIs and by allowing dynamic loading of compiled code that implements a new messaging interface. If required, the transport adapter 614 reformats the instruction payload so that it can be delivered via a particular channel. In particular, an application delivered by SMS may have to be divided into two or more smaller messages due to SMS message size limitations.

The key manager 604 is responsible for generating, distributing and managing the encryption keys issued to the portable device 106, as described below. It also provides encryption and decryption facilities for the message sender 608 and the message receiver 606.

The opt-in manager 610 provides an opt-in, opt-out process to allow client applications 102 select the entities they are willing to receive instruction sets from. This is desirable because the application gateway 104 may be shared by multiple parties and the client application 102 will otherwise execute any received instruction set as long as it is valid. The opt-in manager 610 maintains in the persistent data store 612 associations between parties and the phone numbers (or, in the case of devices other than telephones, other form of address or identifier of the destination device) they are allowed to send applications to. The process for creating these associations can be dynamic to allow users to selectively block or allow instructions from particular parties. For example, Figure 8 shows the message flow for an opt-in process.

At step 802, a party uses the external application 124 executing on the computer system 118 to send a workflow description to the application gateway 104, which at step 804 compiles and formats the instructions in preparation for sending them to a client application 102 that has not opted in. At step 806, the message sender 608 first checks whether the client application 102 has opted in. If not, at step 808 it asks the opt-in manager 610 to determine the opt-in status for this party and this user device. At step 810, the opt-in manager 610 sends an opt-in request message to the user, asking whether they agree to receive applications from this party. If the response is yes, at step 812 the opt-in manager 610 stores this information in the persistent data store 612 and then at step 814 instructs the message sender 608 to send the instruction set at step 816. Otherwise, if the

response is no, then the message sender 608 fails and notifies the party at step 818 that the user has not opted in.

Alternatively, the opt-in process could be performed manually, for example, by using a form that enables the user to directly add entries to the persistent data store 612. Alternatively, an analogous process could be used to opt-out of receiving applications from a particular party.

The message receiver 606 receives messages from the client application 102 and communicates with the transport adapter 614 to receive responses via any of the supported transport channels and protocols, including GPRS, IP network, Bluetooth, and SMS. For example, the instruction set of the interactive system allows instructions to be received by one physical channel/protocol (*e.g.*, SMS), and a corresponding response to be delivered by another (*e.g.*, Bluetooth).

When a message is received, the message receiver 606 first logs the message for audit purposes. Then it checks the authenticity of the message by deciphering the message using the key manager 604, and examining the unique message ID and the party ID to confirm that they match what was sent out.

Once the message authenticity is established, the message receipt is logged for billing and auditing purposes. Finally, the response message is processed as required by the party. This may include emailing the party; logging it to a file for the party to collect; and/or making a request to a third-party application to process the message. The actual method(s) used to process the response message can be specified when calling the API. If the API call does not specify a processing method, then the response is processed using the default method configured for the corresponding developer, determined when the developer establishes an account with the provider of the interactive system.

The persistent storage 612 is a non-volatile storage component that is used by:

(i) the key manager 604 to store the encryption keys for the various mobile devices;

(ii) the message sender 608 to store the addresses of user devices 106 (*e.g.*, phone numbers in the case of the device 106 being a telephone), together with the

delivery mechanisms that each user device 106 supports. It also stores the identifiers of the messages that have been sent out, for verification purposes;

(iii) the message receiver 606, to store received messages for audit and billing purposes; and

(iv) the opt-in manager 610, to store opt-in data representing each user device 106 and the third party applications that are authorised to send instructions to each user device 106.

Encryption keys

As described above, each installed instance of the client application 102 on a user device 106 is identified by a unique client identifier (also referred to herein as the client ID number) that is associated with its phone number. When a client application 102 is first installed on a mobile device 106, a number of private encryption keys are generated and associated with the client ID.

As shown schematically in Figure 9, these encryption keys are then used by the client application 102 to authenticate the payload data and to encrypt the response data. On each payload or response data packet or message, the index of the appropriate encryption key is indicated in the header of the payload.

Figure 10 is a schematic diagram illustrating the message and process flow for generating and updating encryption keys on a client application 102 and an application gateway or backend system 104. The process is initiated by the client application 102 making a secure communication activation request to the application gateway 104 at step 902. In response, the application gateway 104 generates and stores a set of private encryption keys, and associates these with the client ID at step 904. At step 906, the application gateway 104 sends these newly generated private keys to the client application 102. The client application 102 stores the received private keys on the persistent storage 412 at step 908, and returns an acknowledgement to the application gateway 104 at 910, confirming that the private keys have been stored (or updated if the keys had been previously stored). This completes the generation/update steps and secure communication is activated at step 912. This involves encrypting a message payload using one of the private encryption keys, which can be selected at random or on any other basis at step 914. At step 916, the secured payload encrypted with the selected key is sent to the client application 102, together with

a message header specifying the index of the selected encryption key. At step 918, the client application uses the encryption key index indicated in the header to select the appropriate private key, and uses that key to decrypt the payload data at step 918. After performing the application instructions specified by the payload, the client application 102 then encrypts the response at step 920. The response can be encrypted using the same key, as shown in Figure 10, or any other of the stored keys. The secured response is sent to the application gateway 104 at step 922, and the response is decrypted using the appropriate response key at step 924. As will be understood by those skilled in the art, the use of private encryption keys greatly improves the security of communication, and the use of a set of encryption keys, rather than a single key, further increases this security.

When sending a response message, the client application 102 uses the source address of the corresponding payload data by default. This effectively provides multiple client-server communication channels in between the backend 104 and the client application 102. For example, Figure 11 shows an arrangement whereby two instances of the client application 102, a first instance 1002 and a second instance 1004, are in communication with two instances 1006, 1008 of the application gateway 104, via a wireless communications network 110. A message 1010 sent from the first backend system 1008 to the second client application 1004 includes an address 1012 of the first backend system 1008 in the header of the message 1010 so that when the client application 1004 sends the corresponding response 1014, it is addressed to the first backend system 1008.

In contrast, Figure 12 shows the same arrangement whereby a message 1102 also includes the address 1012 of the first backend system 1008. However, workflow instructions contained in the payload data can alter this default behaviour by redirecting the response to another backend server instead. This mechanism is activated by a DIVERT command in the payload data, described further in the Appendix. Specifically, in this message 1102 the payload 1104 includes a divert instruction with the address of the second backend system 1006. Consequently, after the second client application 1004 executes this instruction, the response 1106 is addressed to the second backend system 1006, rather than the first backend system 1008 that originated the message 1102 containing the instructions. Because the second backend system 1006 does not have direct access to the client ID and message ID pair, or the encryption keys for the client application 102, the second backend system 1006 calls an API of the first backend system 1008 to check the integrity and

authenticity of the response data. If the payload was encrypted, then the first backend system 1008 decrypts the payload and sends it back to the second backend system 1006 over a secured communications channel (using SSL, for example). In an alternative embodiment, the encryption keys are stored in a centralised component of the interactive system, and all encryptions and decryptions are performed in this manner.

Communication data payload

The payload exchanged between the client application 102 and the backend system 104 is binary data - a sequence of bytes. The communication channel for this payload can include SMS or Cell Broadcast Service (CBS) messages; IP/TCP data packets (over GPRS, 3G or other type of data networks); and/or Bluetooth data packets.

As shown in Figure 13, each data payload is prefixed with a header 1204 which indicates whether the payload is encrypted with an encryption key. The header data contains the index of the encryption key stored in the client application key-storage, thereby allowing the client application 102 to decrypt the payload data.

As shown in Figure 14, plain payload data (either unencrypted or after being decrypted) contains a series of variable-length data parts that instruct the dynamic workflow execution engine 508 of the client application 102 to construct the user UI workflow.

As shown in Figure 15, each data part includes type 1402 and length 1404 data fields, followed by the actual instruction data 1406. The type field is a single octet or byte that defines the type of workflow instruction that follows. The length indicates the number of octets or bytes of the instructor data 1406.

As described above, the interactive system is able to use one or more of a variety of different communication channels for sending and receiving messages and responses between the application gateway 104 and the client application 102. For most of these different communication channels, the communication itself is straightforward, using the standard methods and libraries available and known to those skilled in the art. However, the interactive system supports message and response delivery via the short message service, or SMS. SMS is defined in the GSM 03.40 specification, which defines an upper limit on the size of each SMS message. Specifically, each SMS message is capable of

containing up to 140 bytes of data, equivalent to 160 ASCII characters when using 7-bit encoding, as shown in Figure 17. The interactive system sends SMS messages including 8-bit (binary) data and including a 7-byte user data header or UDH 1702, as described in the GSM 03.40 specification. The UDH 1702 consists of a length field or UDHL 1704, specifying the length of User Data Header in bytes as specified in GSM 03.40, and a 6-byte User Data Header field 1706 specifying the destination address of the payload data 1708.

The UDH data 1702 - specifying the destination of the binary message - is interpreted by the mobile device to deliver the payload data to the client application 102. Excluding UDH data 1702, each SMS message is capable of carrying 133 bytes of payload data 1708.

If the payload data exceeds this length, the payload data is sent in two or more SMS messages 1804, each message containing up to 127 bytes of payload data 1806, 1808, as shown in Figure 18. These SMS messages 1804 have a section of User Data Header indicating that they all belong to a concatenated message, as described in the GMS 03.40 specification. A byte padding mechanism is used by the backend system 104 and the client application 102 when the payload is sent in multiple SMS messages. In this mechanism, a padding or termination byte 1810 with value 0xFF is appended to the end of each payload data fragment 1806, 1808 when sent out from the backend system 104. The client application 102 removes these padding bytes 1810, which appear as stuffed bytes 1812 in the concatenated payload data before passing the payload data 1814 to the workflow execution engine 408. The byte padding mechanism is used to eliminate problems found in a number of mobile phone models that strip out the last byte of every concatenated data fragment.

The instruction compiler 602 creates the payload data from the compiler output to generate binary SMS messages. Construction of binary messages includes splitting the payload data 1802 into multiple SMS messages 1804 if the data length exceeds the single message capacity of 133 bytes. Figure 19 is a flow diagram showing the steps involved in this process.

As shown in Figure 19, when delivering a message or a response via SMS, at step 1902 a check is performed to determine whether the size of the payload data exceeds 133 bytes. If

not, then at step 1904 a user data header is added, and a single SMS message is composed and sent at step 1906. Alternatively, if the payload length does exceed the maximum size that can be sent in a single SMS message, then at step 1908 a concatenated message identifier is generated, and at step 1910 the number of concatenated messages that are required to accommodate the payload data is determined. Then, a processing loop consisting of steps 1912 to 1920 composes the appropriate number of SMS messages as follows. At step 1912, the next payload portion is selected and copied to the payload of the current SMS message. At step 1914 a user data header is added, including the identifier indicating that the SMS message is part of this SMS message set. At step 1916, a padding or termination byte is appended to the payload data, as described above. Finally, at step 1918 the resulting SMS message is sent. These steps 1912 to 1918 are repeated until the test at step 1920 determines that the last part of the payload data has been sent, and the process then terminates.

Removal of stuffed bytes in the payload data is handled by the client application 102 by searching for the specific stuffed byte octet value (0xFF in this embodiment) and removing it from the payload data, as shown in Figure 20.

Figure 16 is a schematic diagram showing the fifteen different instructions supported by the interactive system, showing the respective type bytes identifying each instruction type, and the structure of the corresponding instruction parameters. Further details on the various instructions are provided in the Appendix.

Dynamic workflow execution engine

The client application 102 presents to the user a number of user interface (UI) widgets 406 as well as executing user-invisible routines. This allows the client application 102 to display information as well as capture device information and/or user inputs.

The UI widgets 406 typically include the following type of user interface components and controls:

(i) Message screen: to show textual information;

(ii) Selection menu: to ask for the user's selection of one of a number of defined choices (*i.e.*, radio buttons);

(iii) Multiple choices: to ask for user's one or more choices (*i.e.*, check boxes);

(iv) Textual input: to retrieve free form text input from the user (textbox);

(v) Numeric or date inputs: to retrieve user input data, restricted by type; and

(vi) Widgets displayed when branching and jumping amongst execution steps.

However, this list of UI widgets 406 and their actual screen layouts can vary depending on the platform (*i.e.*, on each combination of device hardware and operating system software) on which the client application 102 is installed.

The client application 102 implements a workflow execution process 2100, as shown in Figure 21, on each invocation to execute a workflow application. The workflow execution process 2100 begins after the client application 102 is invoked at step 2102, and a test is performed at step 2104 to determine whether the invocation has resulted from the receipt of new payload data from the application gateway 104. If so, then at step 2105 the new payload instructions are retrieved, and then parsed at step 2110. Otherwise, if the invocation was not due to the receipt of new payload data, then a test is performed at step 2106 to determine whether instructions are contained in the instant data storage 410. If so, then the instructions are retrieved from the instant data storage 410 at step 2108, and then parsed at step 2110. Otherwise, another test is performed at step 2132 to determine whether any sets of instructions have been saved as applications in the permanent data storage 412. If not, then at step 2134 an information message is displayed to the user indicating that there are no applications (instant or permanent) in the queue. Once the user acknowledges this information message, or when a corresponding timeout period has elapsed, the client application 102 is terminated. Alternatively, if the permanent data storage 412 contains one or more permanently stored sets of instructions (*i.e.*, applications), then at step 2136 these are displayed to the user, and the process 400 pauses at step 2137, awaiting the user's selection of one of these, or selection of a quit option. If, at step 2138, it is determined that the user has selected the quit option, then the client application 102 terminates. Otherwise, the user has selected a permanently stored set of instructions, and these are retrieved at step 2140, and then parsed at step 2110.

Following parsing of the workflow instructions at step 2110, the first or next workflow instruction is read at step 2112, and executed at step 2114. If it is determined at step 2116 that the instruction is a UI instruction, then the process waits to receive user input at step 2118. Once the user's response has been received, at step 2120 the UI widget

displayed on the screen of the device 106 is removed, and any user input is stored at step 2122. At step 2124, a test is performed to determine whether the instruction was the last in the workflow. If not, then the process loops back to step 2112. Otherwise, once all of the instructions have been executed, then a response message is composed at step 2126, and sent at step 2128. If the workflow instructions executed are stored in the instant data storage 410, then they are deleted at step 2130. This terminates the workflow execution process 2100.

Parsing workflow instructions and response data

The workflow execution engine 408 of the client application 102 interprets the payload data parts and generates the dynamic UI workflow accordingly.

The data parts from the payload data are indexed sequentially when read by the workflow execution engine 408, and, this is also the default order of workflow execution 508. As shown in Figure 22, the response data includes each response in the same order as the corresponding instructions were received and executed. When a workflow instruction is executed and response data is to be retrieved, a parameter name is included in the instruction data, and the user response or system response is associated with this parameter in the response. All the instruction responses are included in the response data when the workflow is completed, as shown in Figure 23.

Jumping and Branching in the workflow

The workflow execution engine 408 provides a mechanism to allow branching and jumping in the sequence of instructions.

Branching

Because an instruction might be involved in different branches through out the workflow, the workflow execution engine 408 differentiates the instruction response data for different branches using branch domains. A branch domain specifies the address of a workflow instruction in the workflow tree. When setting the instruction response data, the response parameter name is prefixed with the corresponding branch domain, separated by a period character. For example, an instruction to retrieve user input for a numeric-valued parameter with the parameter name "number" could be called from two different branch menus: one named "First branch", and the other named "Second branch". In both of these

cases, the instruction returns the same parameter name "number" but with different values. The workflow execution engine 408 associates a branch domain with the parameter name to differentiate the two response values. Thus in this example, the first value is returned as "First branch.number = xxx" and the second value as "Second branch.number = yyy", where "xxx" and "yyy" represent the actual values entered by the user. Figure 25 shows a more complex example where menu selections are nested.

Additionally, the branch domain is appended with a branch name on selection of a branch menu. For example, in an application with two nested branch menus 3902 "Service Request" and 3904 "Water Service" as shown in Figure 39, when the user selects item 3910 "Water" in menu 3902, and then selects item 3912 "Pipe Burst" in the subsequent branch menu 3904 "Water Service", and then fills out 3914 with "John Doe" in the text input screen 3906 "Your name", the client application 102 will internally send the response as "Water.Pipe burst.name=John Doe". When the BRANCH_BACK command is executed, the previous branch name is removed. The workflow execution engine 408 uses a branch name stack to maintain the order of branch names as they are selected.

For usability reasons, when working with a multiple branch menu, it is important for the user to know whether or not a branch has already been visited by the user. To this end, the workflow execution engine 408 indicates visited branch menu items by displaying an image adjacent to those branches to indicate that they have already been visited by the user. For example, as shown in Figure 27.

When the user has visited user input screen 2702 to enter data 1, an image icon 2706 is displayed adjacent to the first branch menu item 2704 is marked with distinct. This allows user to visually distinguish those parts of the workflow that have been visited from those parts that have not been visited. Alternatively, the visited branches could be displayed in a different colour, as used by web browsers to indicate that a hyperlink has been visited.

Backward navigation

As shown in Figure 28, all of the user interface screens include a "Back" navigation button 2802 to allow the user to return to the previous screen within the workflow. The position of this back button can change depending on the specific mobile device platform executing

the client application 102. As shown in Figure 29, the workflow execution engine 408 maintains an ordered list or stack of instructions that cause a change in the screen or display, and selection of the "Back" button causes the execution to return to the previous instruction.

Sending a workflow description to the Instruction Compiler

As described above, a developer 116 can send a workflow description to the instruction compiler 602 of the application gateway 104 by submitting programming instructions written in the programming language supported by the instruction compiler 602, using a hypertext transport protocol (HTTP) interface of the instruction compiler 602. For example, Figure 30 is a screenshot of an HTML webpage generated by the application gateway 104. The webpage includes a scrollable text box 3002 into which the developer 118 can directly enter commands in the scripting language, and a compile button 3004 which, when pressed, submits the text in the scrollable text box 3002 to the instruction compiler 602 for compilation.

The scripting language of the interactive systems is a high level language for describing the workflow of an interactive application. It is similar in vein to BASIC and can be learnt quickly by a programmer who has a basic knowledge in programming.

Alternatively, a workflow description can be sent to the instruction compiler 602 by invoking API calls to the application gateway API 616. For example, Figure 31 shows a source code listing of a J2ME function `SendWorkflowRequest` that is used to generate and send workflow instructions to the mobile telephone 106. In this example, the workflow instructions are to display booking details to the user 120 and then retrieve the user's response indicating whether the user 120 accepts or rejects the booking, together with the user's name and telephone number. The workflow API is first initialised by creating (at 3102) a new J2ME Command() object named `WorkflowCommand`. A workflow header, as described below, is then added at 3104. Workflow instructions are then added in the order of desired execution by calling APIs that are provided as methods of the `WorkflowCommand` object. Each type of workflow instruction is added by calling a corresponding API function with a set of parameters. For example, the object method `AddInfoMessage` is used (at 3106) to add an instruction that displays a screen of

information to the user. The first argument to this method provides a title for the screen, and the second argument provides the actual text information that is displayed. Similarly, the method `AddSingleMenu` adds (at 3108) an instruction that displays a single-level menu (*i.e.*, radio buttons) to the user, allowing the user to select one item from a list of items provided as a parameter to the method. In this example, the two items are displayed as "Accept", and "Reject", and the user's response indicates whether the user 120 accepts or rejects the booking.

The method `AddUserInputCmd (at 3110 and 3112)` displays a text string to the user, together with a textbox, prompting the user to enter an appropriate input value. The first parameter to this function finds the name of the parameter that will be associated with the returned input value. The second argument provides a string that is displayed to the user, and a third argument allows the developer to restrict the type of input; for example, to a phone number, email address, and so on.

Finally, the `AddRedirectHeader` method (at 3114) defines a return address or phone number to which the response will be redirected, as described above. The communication channel to be used (*e.g.*, whether by SMS, IP network, Bluetooth, etc) is also specified in the header.

Once the workflow instructions are added, the workflow API is called again (at 3116) to compile the instructions and build the payload data to be sent to the client application. The workflow API is called as many times as needed (at 3118) to send multiple messages if required.

Scripting Language Overview

- Instructions are written line by line.
- Comment lines start with //
- Label lines start with #
- String parameters are delimited by double quote characters ""

Workflow-programming Structure

Commands are processed sequentially line by line. Three instructions are provided to create tree structures of the workflow: BRANCH_TO, BRANCH_BACK, and GOTO. BRANCH_TO and BRANCH_BACK are used in combination to create a subroutine for the compiled program. GOTO is a jump instruction that allows program execution to jump to a specified line in the script. Comment and blank lines are ignored by the instruction compiler 602.

Command line syntax

A command is a line in the script which has the following structure:

<Command Name> <String Parameter> <String Parameter> <Label>

Where:

- <Command Name> is a command.
- <String Parameter> is a qualified string value, *i.e.*, delimited by double quote characters. For example, "User name" is a string parameter. There can be more than one string parameter in each command.
- <Label> is the name of the label that is associated with the command. Labels can only be used with the GOTO command and the ITEM command when used in conjunction with BRANCH_TO command.

Comment

There is no block comment in the language. Comment lines are lines that start with // (two forward slash characters followed by a space character).

Example:

// this is a comment line

Label

A label is a way to mark a line number so that it can be referred to in GOTO and BRANCH_TO 's ITEM commands. A label line starts with # (hash) character, followed by a space character. The label name is the next word from the # character.

Example:

For label START, the line looks like this:

START

The label name is mapped to the index (*i.e.*, relative position in the script) of the command immediately following the label line.

Labels in a script must be unique, a compile error occurs if a duplicate label is detected. All labels are parsed in the first pass of the compiler, building a mapping of label and command index to be used in the second pass.

Backward navigation

As described above, a "Back" navigation button is attached to all displayed screens by default. This button allows backward navigation of the workflow executed on the user device 106. On most mobile phone platforms, this "Back" button is mapped to the right action key. However, this can change depending on the type of phone.

Tree navigation

A combination of the BRANCH_TO command, labels, and the BRANCH_BACK command allows the workflow to support a tree like execution structure, as shown in the source code listing of Figure 32 and the resulting display screens of Figure 33. A detailed description is provided below. When a user is navigating thought workflow screens, the state of each screen (item selection and user inputs) is not remembered.

Example

The following is a source code listing that is used to generate an interactive application for execution on a user device such as the mobile telephone 106. The source code defines a workflow that allows the user 120 of the mobile telephone 106 to generate a service request for water, electricity, and/or gas services. The listing is arranged in four groups of commands or paragraphs under respective labels. The first paragraph, labeled START, results in display of a main screen 3402, as shown in Figure 34. The BRANCH_TO command has two parameters. The first, "serv" defines a branch name for this branch, and the second parameter, "Service Request" defines the title that is displayed at the top of the main screen 3402. The subsequent three commands define items that can be selected by the user to invoke corresponding workflow branches. For example, the first ITEM command has two parameters. The first parameter, "Water", defines the text 3404 that is displayed on the main screen 3402, and that can be selected to invoke the corresponding workflow branch. The second parameter, in this case "WATER", is a label of the corresponding

workflow branch, in this case referring to the second group or paragraph of commands grouped under that label. Thus if the user navigates the main screen 3402 to select the first item 3404, the workflow jumps to the SELECT ITEMS, causing display of a water service selection screen 3406. In this case, the three items are simply menu selections (rather than workflow branches), and thus selection of any one of these items causes the appropriate parameter, in this case named "water" to be assigned a value defined with the corresponding item. For example, if the user selects the second item, "Leaking" 3408, then the parameter "water" is assigned the value "Leaking". Once this item has been selected, the workflow proceeds to the following command, which in this case is the BRANCH_BACK command, which returns control to the main screen 3402.

In this manner, the user can select the Electricity item 3410 to branch to the ELECTRICITY workflow, resulting in display of a Electricity service screen 3412. Similarly, the user can select the "Gas" request item 3414 to cause a Gas service screen 3416 to be displayed. Once the user is satisfied with the service requests thus defined, selection of the Next button 3418, or the OK button 3420 causes execution to continue to execute in this example the command "GOTO CONTACTS", which causes the workflow to jump to the command following the CONTACTS label, being in this case an INPUT command displaying a name input screen 3422, and subsequently a Contact number screen 3424. Once the OK button 3426 on the Contact numbers screen 3424 has been selected, a MESSAGE command causes display of a Service Info screen 3428 providing informational feedback to the user, in this case confirming that the service request will or has been sent to an appropriate party for processing the user's request.

```
// Start of program
# START
BRANCH_TO     "serv" "Service Request"
ITEM          "Water" WATER
ITEM          "Electricity" ELECTRICITY
ITEM          "Gas" GAS
GOTO          CONTACTS

# WATER
SELECT        "water" "Water service"
```

```
ITEM            "Pipe Burst"
ITEM            "Leaking"
ITEM            "New connection"
BRANCH_BACK

# ELECTRICITY
SELECT      "elect" "Electricity service"
ITEM            "Fire"
ITEM            "New connection"
ITEM            "Disconnection"
BRANCH_BACK

# GAS
SELECT      "gas" "Gas service"
ITEM            "Leaking"
ITEM            "New connection"
ITEM            "Fire"
BRANCH_BACK

// This is like a subroutine
# CONTACTS
INPUT           "name" "Your Name" ANY
INPUT           "phone" "Contact Number" NUMERIC
// message is sent here
//# END
MESSAGE     "Service Info" "Your request will be sent to XXXX"
```

Script commands and syntax

HEADER command

The HEADER command is used to include a specified piece of text at the beginning of the response message when the workflow has been executed. This command is invisible to the

user of the user device. This command is used as a context identifier for server-client conversation.

There can be multiple header commands in the script. When using the HEADER command in conjunction with the BRANCH_TO command, different response message prefixes can be set, based on the user's selection.

Syntax

HEADER <header>

- <header> is a string parameter to be prepended to the response text message.

Example

HEADER "timesheet"

Response

<header> is attached to the beginning of the response message. If there are multiple headers to be included in the response message, the response headers are prepended based on their execution order in the workflow.

DIVERT command

The DIVERT command is used to redirect a response message to a telephone number or address different from that of the source of the original instructions. Normally, the response message is sent back to the source address of the payload, but the response message can be sent back to another number instead by including a DIVERT command in the workflow. This command is invisible to the user. There can be multiple DIVERT commands in the script, but the last one that is executed in the workflow takes effect. When combining this command with the BRANCH_TO Command, the workflow can send a response message to a source number selected by the user.

Syntax

DIVERT <address>

- <address> is a string parameter representing the mobile number of the redirected address.

Example

DIVERT "+61418366896"

MESSAGE command

MESSAGE command shows a message with a title and message content to the user.

Syntax

MESSAGE <title> <message content>

- <title> is a string parameter for of the title of the message to be displayed.
- <message content> is a string parameter.

The end result is display of a screen as shown in Figure 35.

Example

MESSAGE "Hello" "Hello world"

Response

This GUI screen does not collect any user input and no response data is associated with it.

INPUT command

This command displays a GUI screen with a text input box 3602 to the user to retrieve user inputs, as shown in Figure 36. A parameter name is provided in the command to set the name of the user input data when included in the response message. A default input value can be provided as an input parameter. If desired, the user input data can be restricted to a certain types such as numeric, decimal or a phone number. However, the implementation of user input restriction depends on the capability of the user device executing the client application 102.

Syntax

INPUT<return parameter> <label> <type> <default value>

- <return parameter> is a string parameter for the name of the entered value to be set in the return message.
- <label> is the title of the input text box
- <type> is the type of the input to be captured, these types are available:
  - ANY
  - EMAILADDR
  - NUMERIC

- PHONENUMBER
- URL
- DECIMAL

- <default value> is an optional string parameter to be set to the input text box when the screen is visible to the user. If omitted, the default value of the input text box is left empty.

Response

User input data is included in a response message associated with a parameter name specified in the corresponding instruction. If the INPUT command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<return parameter>=<value> (without domain path)

<domain path>.<return parameter>=<value>

Where:

- <value> is a string value that user enters. This can be an empty value.
- <domain path> is the path of branches that lead to this INPUT command in the workflow.

GAUSS command

This command results in the display of an interactive screen having a slider or "gauss" control 3702 to prompt the user to provide corresponding response data, as shown in Figure 37. The user is able to slide the slider control from a minimum value to a maximum value specified on the command line. The resulting data is included in the response message associated with the parameter name given.

Syntax

GAUSS <parameter name> <minimum value> <maximum value> <default value>

- <parameter name> is a string parameter for the name of the gauss value to be set in the return message.
- <minimum value> is the minimum value the user can select.
- <maximum value> is the maximum value the user can select

- <default value> is the default value if the user does not select any value. This parameter is optional so if it is not present, the default value is empty.

Example

GAUSS "temper" "1" "10" "5"

Response

If this command is executed in a branch routine (see BRANCH_TO command) then any domain path applicable will be prefixed to the parameter name.

<parameter name>=<value> (without domain path)

<domain path>.<parameter name>=<value>

GOTO command

This command allows the workflow execution engine 406 to jump to a specific workflow instruction, rather than proceed to the next instruction in sequence. A parameter of this command is the label of the instruction for the workflow execution to be directed to. There is no user screen or response data associated with this instruction.

Syntax

GOTO <label>

- <label> is the label name indicating the index the command that the workflow execution jumps to after executing this command.

Example

```
....
GOTO Hello  // The program jumps to message hello world after executing this command.
...
...
# Hello
MESSAGE "Hello" "Hello world"
...
```

SELECT, SELECT_MULTI command

As shown in Figure 38, these commands display a screen with a list of items to select from. The SELECT command allows single item selection, and the SELECT_MULTI command allows multiple item selection screen. The user selection is included in the response message identified by the parameter name. In case of multiple selection list, the selected values are separated by a delimiter character in the response value data.

Syntax

SELECT or SELECT_MULTI command is followed by ITEM definitions (one per line).

```
SELECT  <parameter name> <title>
ITEM    <item name>
ITEM    <item name>
ITEM    <item name>

SELECT_MULTI < parameter name> <title>
ITEM    <item name>
```

ITEM <item name>
ITEM <item name>

Where:

- < parameter name > is a string parameter specifying the return parameter id for the SELECT screen.
- <title> is a string parameter specifying the title of the screen.
- <item name> is a string parameter specifying the item to be displayed on the screen.

Example

```
// This example allows the mobile user to select one of the option listed
SELECT "tsk" "Select task"
ITEM "Administration"
ITEM "Service desk"
ITEM "Client meeting"

// This example allows mobile user to select one or many of user names in the list
SELECT_MULTI "name" "Select users"
ITEM "User 1"
ITEM "User 2"
ITEM "User 3"
```

For multiple select command, each of the items in the select list is displayed adjacent to an icon that indicates whether or not the item has been selected by the user. On most mobile devices, a "Mark" button is displayed to allow user to mark the selection of the highlighted item. A "Next" button is also attached to this screen to allow the user to navigate to the next workflow instruction. On some mobile device platforms, the Next button is mapped directly to one of the mobile phone buttons.

Response

SELECT command:

<parameter name>=<item>

SELECT_MULTI command:

< parameter name >=<item>;<item>;<item>

Where:

- <item> is the item name as selected

The multiple select response can be empty.

BRANCH_TO command

This command provides users a list of items to select, and on selection of an item, execution of the workflow is branched to the specified command. The behavior of this screen is similar to the SELECT screen described above. Once the workflow execution starts executing from the new target instruction, it follows the default sequential order. When the BRANCH_BACK command is executed, the workflow execution engine returns to the previous BRANCH_TO command to execute. However, the BRANCH_TO command does not require a BRANCH_BACK command to operate. The workflow can consequently branch to the last command without returning to the branch menu.

To progress to the next screen from a BRANCH_TO command, a "Next" button is provided. On some phones, this button is mapped to one of the phone keys on the mobile device. On most phones however, this button is mapped to a soft-key named "Next" when the user select Options on the BRANCH_TO screen (similar to SELECT_MULTI command).

There is no specific user value attached to this screen in the response message. The selected branch item is however appended to the branch domain path. This domain path is then appended to the parameter name of any input screens being executed in the branch target.

Syntax

BRANCH_TO command is followed by ITEM definitions (one per line).

```
BRANCH_TO    <parameter name> <title>
ITEM         <item> <label>
ITEM         <item > <label>
ITEM         <item > <label>
```

Where:

- < parameter name > is a string parameter specifying the return parameter id for the BRANCH_TO screen.
- <title> is a string parameter specifying the title of the screen.
- <item > is a string parameter specifying the item to be displayed on the screen.
- <label> is a valid label name as specified in the workflow with "#" character.

Examples

```
...
# EnterBetAmount
INPUT "bet" "Enter bet amount" DECIMAL
BRANCH_BACK
....
# SelectBetAmount
SELECT "bet" "Select bet amount in dollars"
ITEM "100"
ITEM "200"
ITEM "300"
BRANCH_BACK
....
BRANCH_TO "b" "Select team to bet"
ITEM "Melbourne" EnterBetAmount
ITEM "Geelong" SelectBetAmount
GOTO END
...
# END
MESSAGE "Info" "Please select Yes to allow response message to be sent"
```

Response

- The domain path is appended with <item> selected in the branch menu.
- This domain path is then appended to the parameter name of any input screen executed in the branch target. In the example script, the "bet" amount parameter name when appearing in the response message is: Melbourne.bet=<bet value>.

BRANCH_BACK command

This command is invisible to the user, it provides the capability to navigate back from branching. A workflow could have multiple branches wired up and the result is a tree like structure. BRANCH_BACK command allows navigation upwards in this tree structure. Combination of label and BRANCH_BACK command allows combining a group of workflow commands in to a routine, which can be referred to multiple times during the workflow execution.

Syntax

BRANCH_BACK

STORE_PERMANENT command

This command instructs the workflow execution to store the whole payload data to persistent storage. A title is set in the parameter of this command allows the client application to display the stored payload data to the user. This command does not result in any user data in the response message.

Syntax

STORE_PERMANENT <title>

Where:

- <title> is a string parameter indicating the title of workflow payload data to be displayed in the persistent list. This persistent list is displayed to the user when the client application is started manually by the user and no instant payload data is waiting to be executed.

Example

STORE_PERMANENT "Message one"

CLEAR_PERMANENT command

This command clears all the persistent workflow payload data previously saved by STORE_PERMANENT command. Execution of this command does not result in any data in the response message.

Syntax

CLEAR_PERMANENT

EXECUTE command

This command makes a request to the mobile device operating system to retrieve an URL address. The results could be making a phone call or launching the internet browser on the phone to the specified URL address. Behavior of this command might varies across different device models due to device capabilities.

Syntax

EXECUTE <url_address>

Where:

- <url_address> is a string parameter describing the URL address of the request to be sent to the J2ME platform.

Example

To make a mobile phone call to +61418366896 mobile number

EXECUTE "tel:+61418366896"

To launch the internet browser on the mobile phone to access ACME mobile website

EXECUTE "http://mobile.acme.com"

Response

If making a mobile phone call is required, the mobile device will ask user if a mobile phone call can be made. If launching of the internet browser is required, the application will ask for the user's permission to open the internet connection to the specified URL.

CONFIGURATION command

The response message is constructed from the user/system data. A number of default delimiter characters are used to separate the data parts as well as name-value separator. This command when included in the payload data can change the delimiter characters of the response message as well as specifying whether or not the name part is included in the response message.

Syntax

CONFIGURATION <configuration_string>

Where <configuration_string> is composed of configuration characters:

- 1st character: Include parameter in the response, if set to '0', the response message only has values, set to '1', the response message has Name=Value
- 2nd character: Response part delimiter, the default is ','
- 3rd character: Equal character, the default is '='
- 4th character: Multiple selection options, the default is ';'
- 5th character: Screen path delimiter, the default is '.'

Example

CONFIGURATION "0,=;."

This configuration command instructs the workflow execution to exclude parameter names from the response message.

SYSTEM_PROPERTY command

This command instructs the workflow execution to read a system property and return the result in the response. The parameter name that is associated with the response data is the system property if parameter name is omitted.

Syntax

SYSTEM_PROPERTY <property_name> <parameter name>

Where:

- <property_name> is the system property to be read. On the J2ME platform, examples of these properties are:
  - microedition.profiles
  - microedition.configuration
- <parameter name> is an optional string parameter. If omitted, property name is used as parameter name in the response instead.

Examples

SYSTEM_PROPERTY "microedition.profiles"

SYSTEM_PROPERTY "microedition.profiles" "midp"

Response

The value of the system property is included in the response message as name=value pair. All the rules applied to the name-value pairs are applied. These include changing of delimiter parameters and whether or not to include the name part in the response message.

<system property>=<value> (if parameter name is omitted)

<parameter name>=<value> (if parameter name is present)

NOP command

This is a no-operation command. It is useful when used in conjunction with labeling.

Syntax

NOP

SET_KEYS command

A command to set the encryption key specified by the index of the key on the mobile device.

Syntax

SET_KEYS <key_index> <key>

Where <key_index> is a string parameter indicating the index of the key to be set on the client application 102. <key> is a string parameter containing the actual key to be updated.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

It will be apparent from the description above that the interactive system and process described herein allow a developer to dynamically send on demand customisable workflow instructions to one or more user devices 106 such as mobile telephones. The generation, secure delivery, execution, and secure return of response data to the developer are all handled transparently by the interactive system, thus hiding all the details of these aspects from the developer, greatly simplifying the provision of interactive applications and quasi-real-time interactions with one or more users. The provision of workflow instructions via

SMS is particularly advantageous as it can be assumed to be supported by all mobile telephones available today. Moreover, since the SMS communications are all managed by the interactive system, any premium SMS services that may be required can be established by the operator of the interactive system, thus freeing the developer from needing to establish their own independent premium SMS services. This greatly simplifies the provision of new interactive applications, and also allows the operator of the interactive system to provide these services at a lower cost by leveraging the substantial volume of SMS traffic resulting from the aggregation of SMS traffic or all developers using the interactive system.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method of delivering an instruction to a mobile user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

2. A method as defined by claim 1 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow coded in a high level programming or scripting language.

3. A method as defined by either of claims 1 or 2 wherein the step of receiving the interactive workflow includes the step of receiving the interactive workflow from an external or third party.

4. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending a set of instructions for execution by an application installed on the mobile user device.

5. A method as defined by claim 4 wherein the step of sending the set of instructions includes the step of sending the set of instructions for the device to interact with a user of the mobile user device.

6. A method as defined by claim 5 wherein the step of sending the message includes the step of sending a unique message identifier.

7. A method as defined by claim 6 further comprising the step of the mobile user device receiving the set of instructions and the unique message identifier.

8. A method as defined by claim 7 wherein the step of the mobile user device receiving the set of instructions and the unique message identifier includes the step of receiving the set of instructions for translation to mobile user device system codes by a workflow execution engine component of the application.

9. A method as defined by either of the claims 7 or 8 further comprising the step of receiving a response to the instruction from the mobile user device.

10. A method as defined by claim 9 wherein the step of receiving a response includes the step of receiving a response identifier from the device.

11. A method as defined by claim 10 wherein the method comprises the step of comparing the unique message identifier and the response identifier to confirm the authenticity of the received message.

12. A method as defined by any one of the preceding claims wherein the step of translating the instruction includes tailoring the instruction to a device operating system.

13. A method as defined by any one of the preceding claims wherein the mobile user device is one of a plurality of mobile user devices and the method also comprises the step of receiving a specification of the mobile user device from a database comprising respective specifications for the plurality of user devices.

14. A method as defined by claim 13 wherein the step of translating the interactive workflow includes tailoring the instruction to the specification.

15. A method as defined by any one of the preceding claims wherein the step of sending the message includes one or more preliminary steps of compressing, encoding and encrypting the instruction.

16. A method as defined by any one of the preceding claims wherein the step of sending the message includes the step of sending the message via a Short Message Service (SMS) of a cellular network.

17. A method as defined by claim 16 wherein the step of sending the message via SMS includes the step of splitting the message into a plurality of messages to comply with one or more standards of the SMS.

18. A method as defined by any one of the claims 1-15 wherein the step of sending the message includes one or more of the steps of sending the message via a Cell Broadcast Service (CBS) of a cellular network, sending the message as an IP/TCP data packet over a GPRS or 3G network, and sending the message as a data packet over a Bluetooth connection.

19. A method as defined by any one of the preceding claims also including the step of checking if the mobile user device is willing to receive the instruction derived from the interactive workflow.

20. A method as defined by claim 19 wherein the step of checking involves sending a request to the user of the mobile user device to accept the instruction derived from the interactive workflow.

21. A method as defined by claim 3 wherein the step of receiving the interactive workflow includes the preliminary step of receiving a request for an Application Programming Interface (API) from the external or third party.

22. A method as defined by claim 21 wherein the step of receiving the interactive workflow includes the preliminary step of opening an Application Programming Interface.

23. A method as defined by any one of the preceding claims also comprising the step of issuing a command to the device to update or delete a sequence of instructions saved to a permanent data store on the mobile user device.

24. Computer software comprising executable directions for delivering an instruction to a mobile user device connected to a network, the directions comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the mobile user device; and

sending a message including the instruction to the mobile user device.

25. A method of delivering an instruction to an application installed on a user device connected to a network, the method comprising the steps of:

receiving an interactive workflow;

translating the interactive workflow into the instruction in a form executable by the application; and

sending a message including the instruction to the application at the user device.

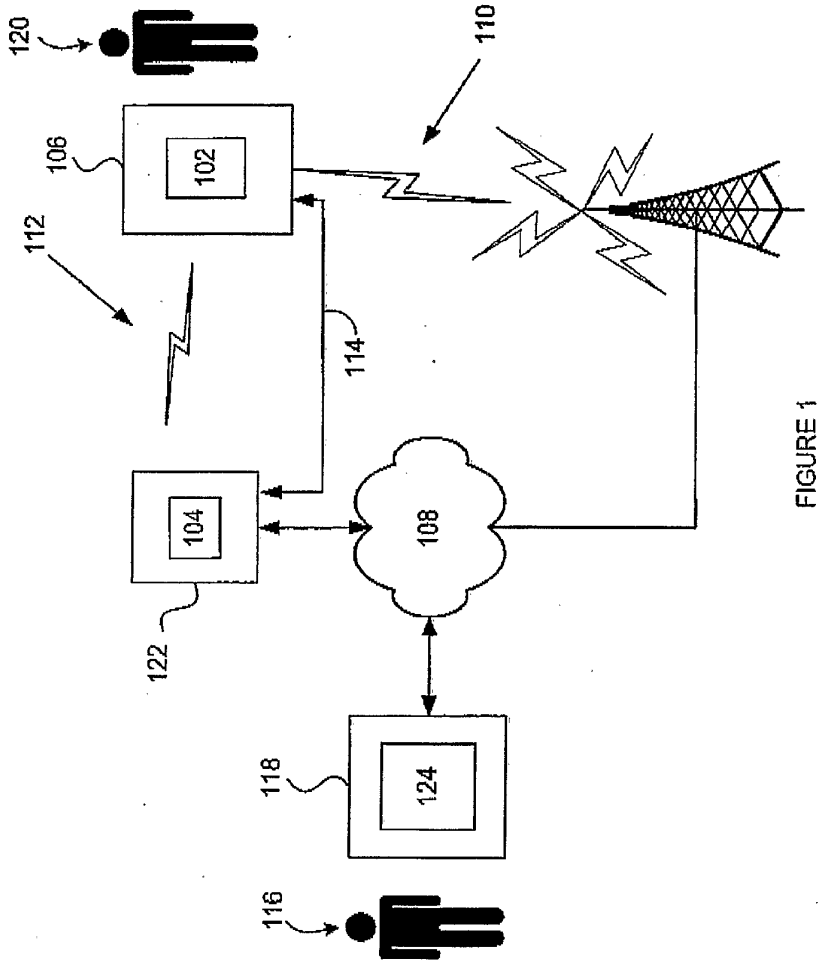


FIGURE 1

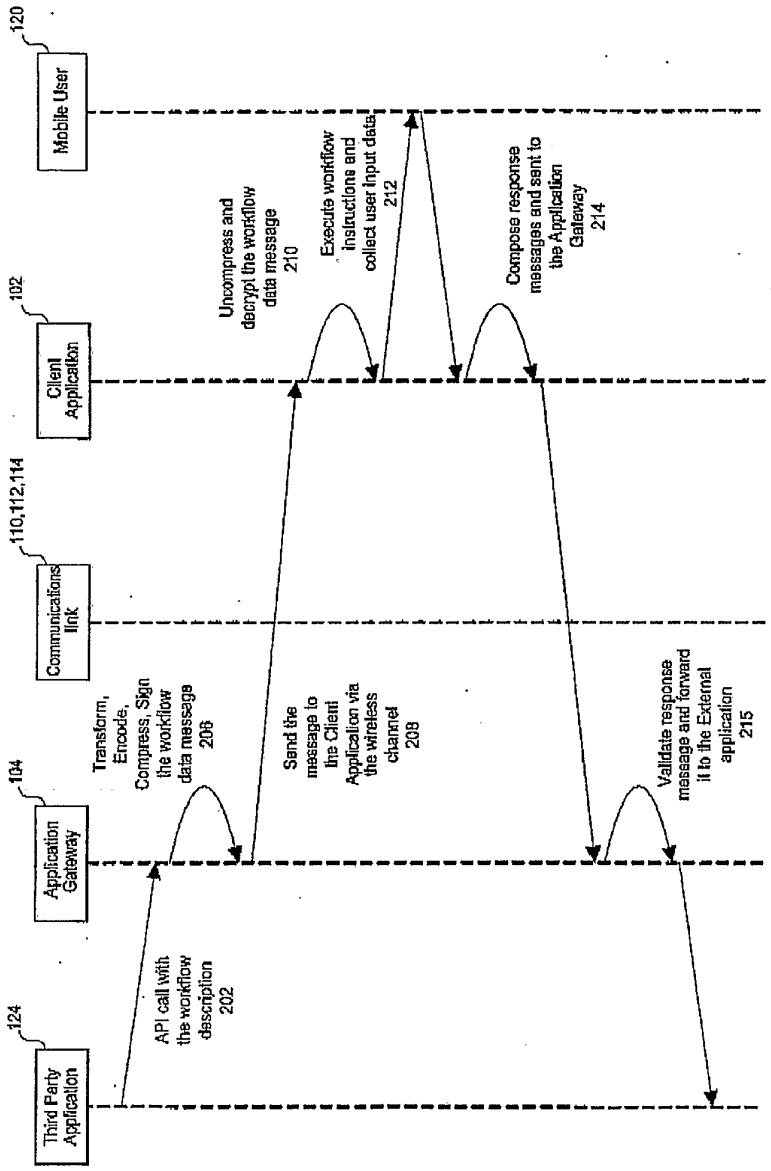

120
Mobile User
102
Client Application
110,112,114
Communications link
104
Application Gateway
124
Third Party Application
API call with the workflow description 202
Transform, Encode, Compress, Sign the workflow data message 206
Send the message to the Client Application via the wireless channel 208
Uncompress and decrypt the workflow data message 210
Execute workflow instructions and collect user input data 212
Compose response messages and sent to the Application Gateway 214
Validate response message and forward it to the External application 215

FIGURE 2

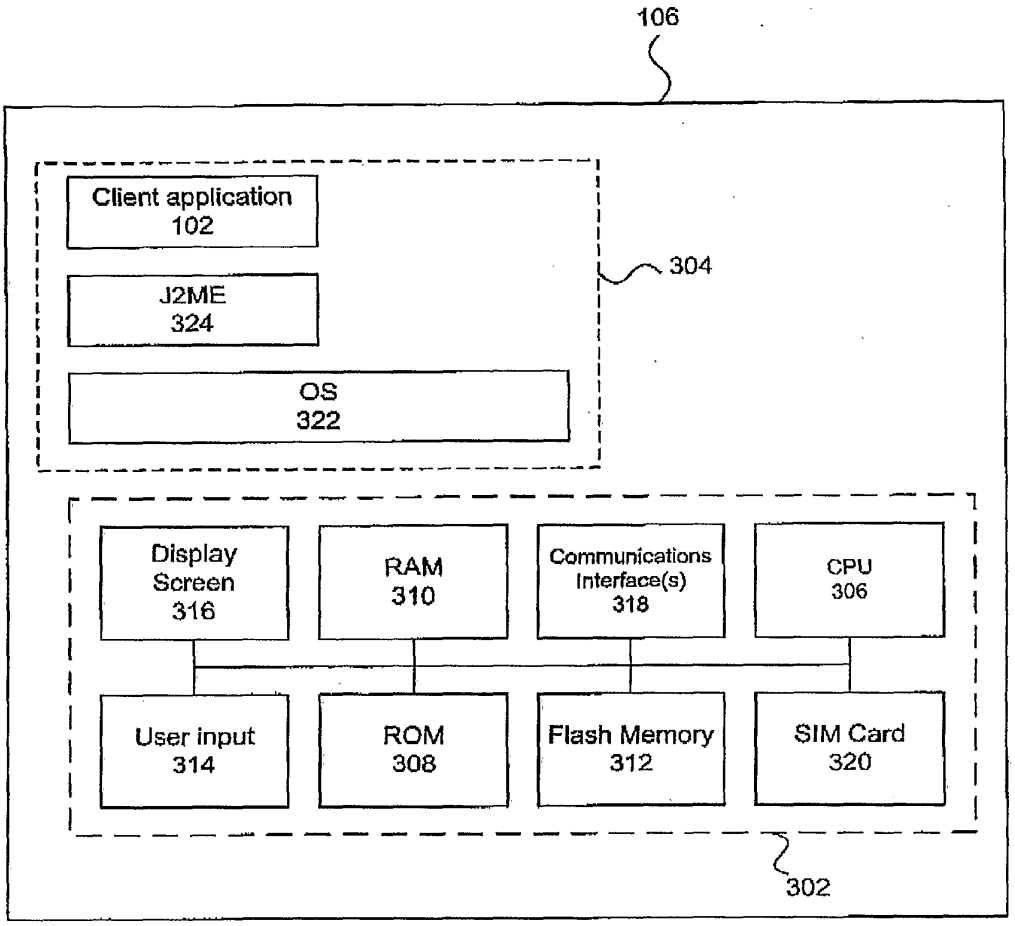

106
Client application
102
J2ME
324
OS
322
304
Display
Screen
316
RAM
310
Communications
Interface(s)
318
CPU
306
User input
314
ROM
308
Flash Memory
312
SIM Card
320
302

FIGURE 3

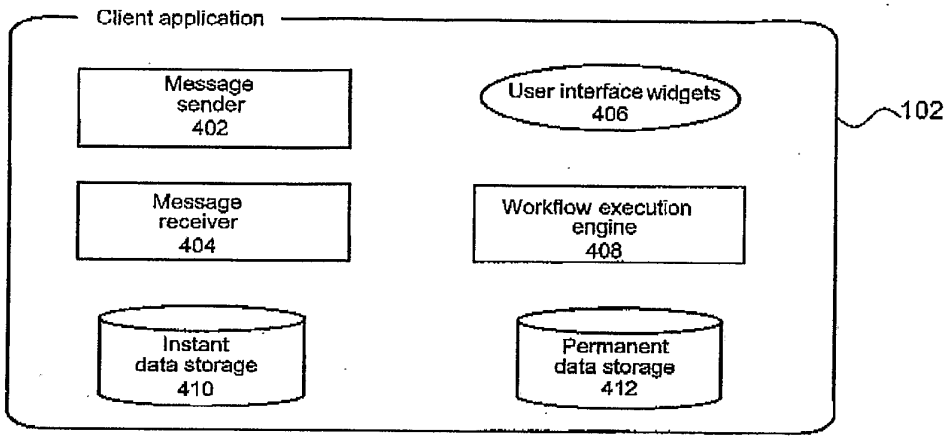


FIGURE 4



FIGURE 5

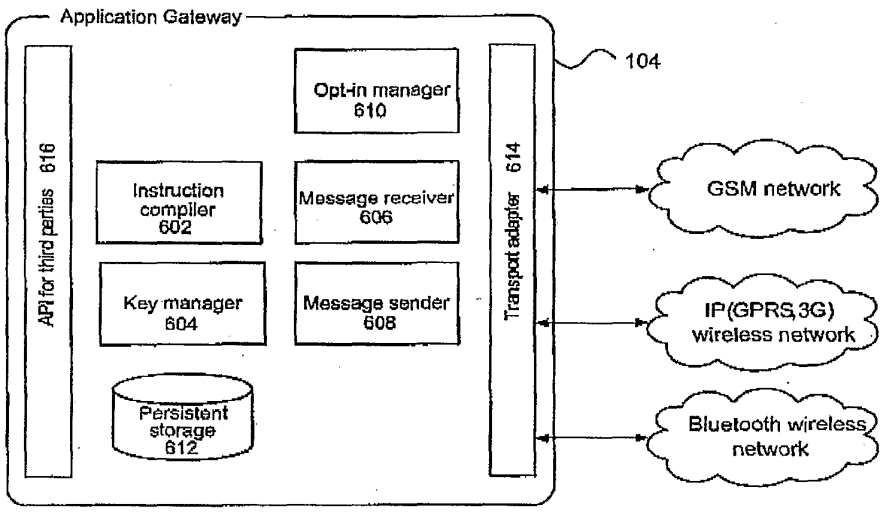

Application Gateway
API for third parties 616
Instruction compiler 602
Key manager 604
Persistent storage 612
Opt-in manager 610
Message receiver 606
Message sender 608
Transport adapter 614
104
GSM network
IP(GPRS,3G) wireless network
Bluetooth wireless network

FIGURE 6

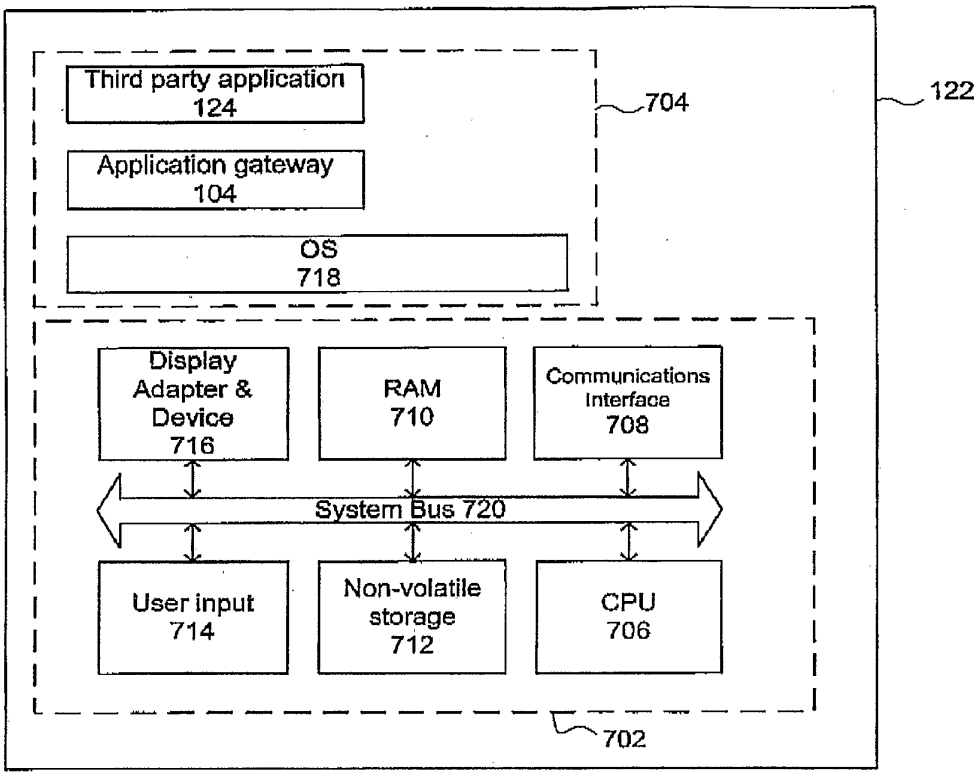

Third party application
124
Application gateway
104
OS
718
704
122
Display
Adapter &
Device
716
RAM
710
Communications
Interface
708
System Bus 720
User input
714
Non-volatile
storage
712
CPU
706
702

FIGURE 7

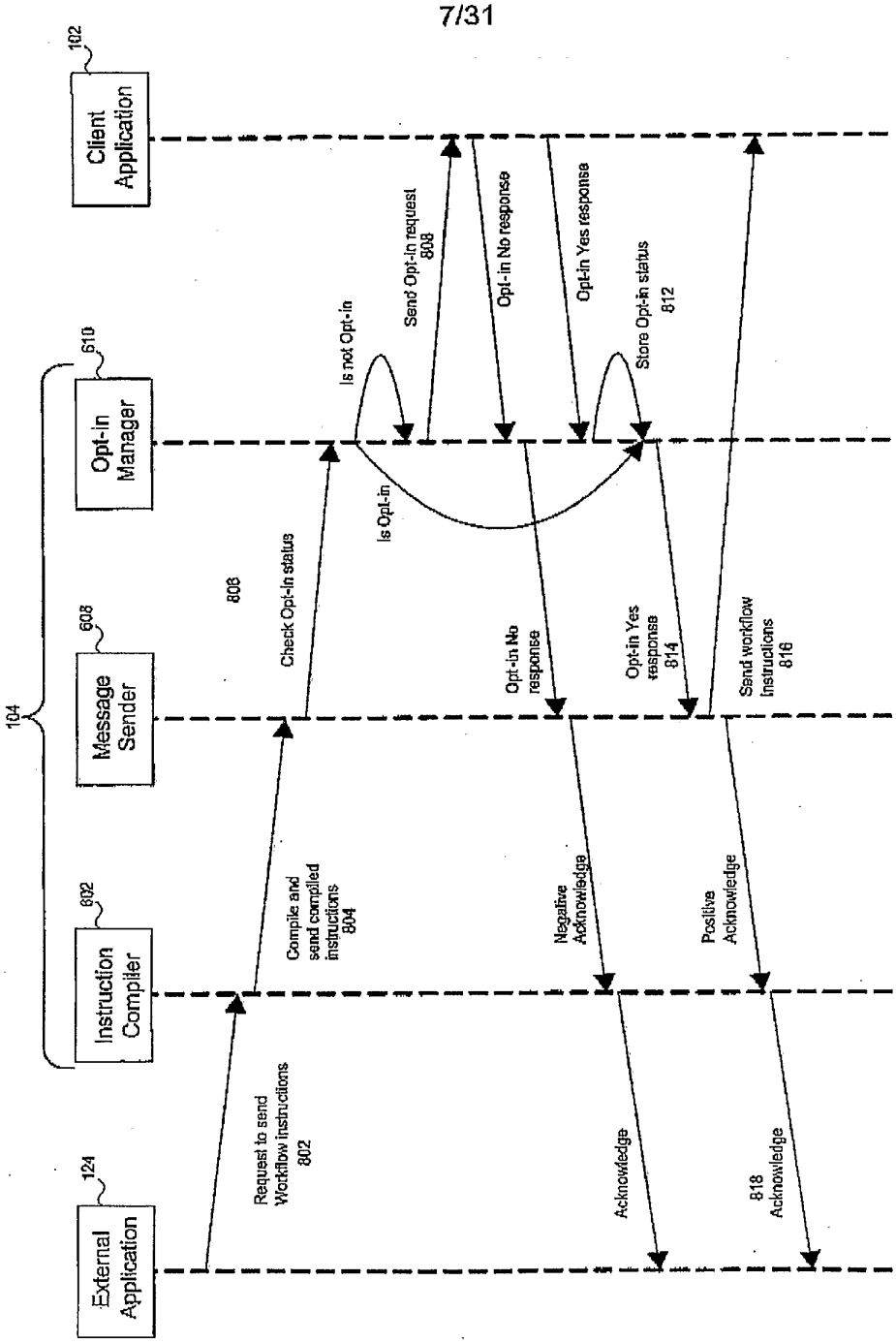

102
Client Application
610
Opt-in Manager
608
Message Sender
602
Instruction Compiler
124
External Application
104
Request to send Workflow instructions 802
Compile and send compiled instructions 804
Check Opt-in status 806
Is not Opt-in
Send Opt-in request 808
Opt-in No response
Opt-in Yes response
Store Opt-in status 812
Is Opt-in
Opt-in No response
Opt-in Yes response 814
Send workflow instructions 816
Negative Acknowledge
Positive Acknowledge
Acknowledge
818 Acknowledge

Figure 8

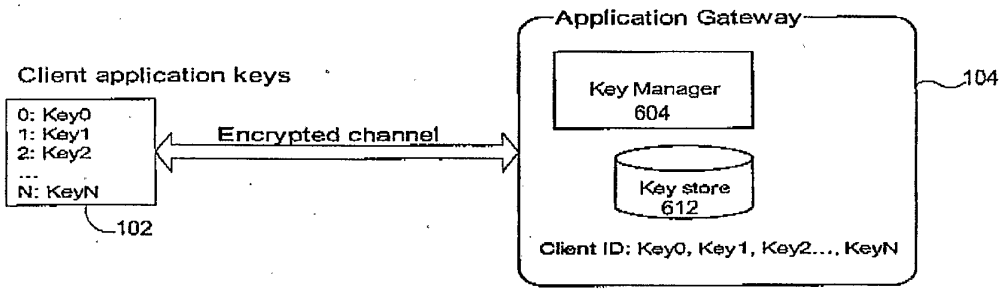

Application Gateway
Client application keys
0: Key0
1: Key1
2: Key2
...
N: KeyN
Encrypted channel
Key Manager
604
Key store
612
Client ID: Key0, Key1, Key2..., KeyN
102
104

FIGURE 9

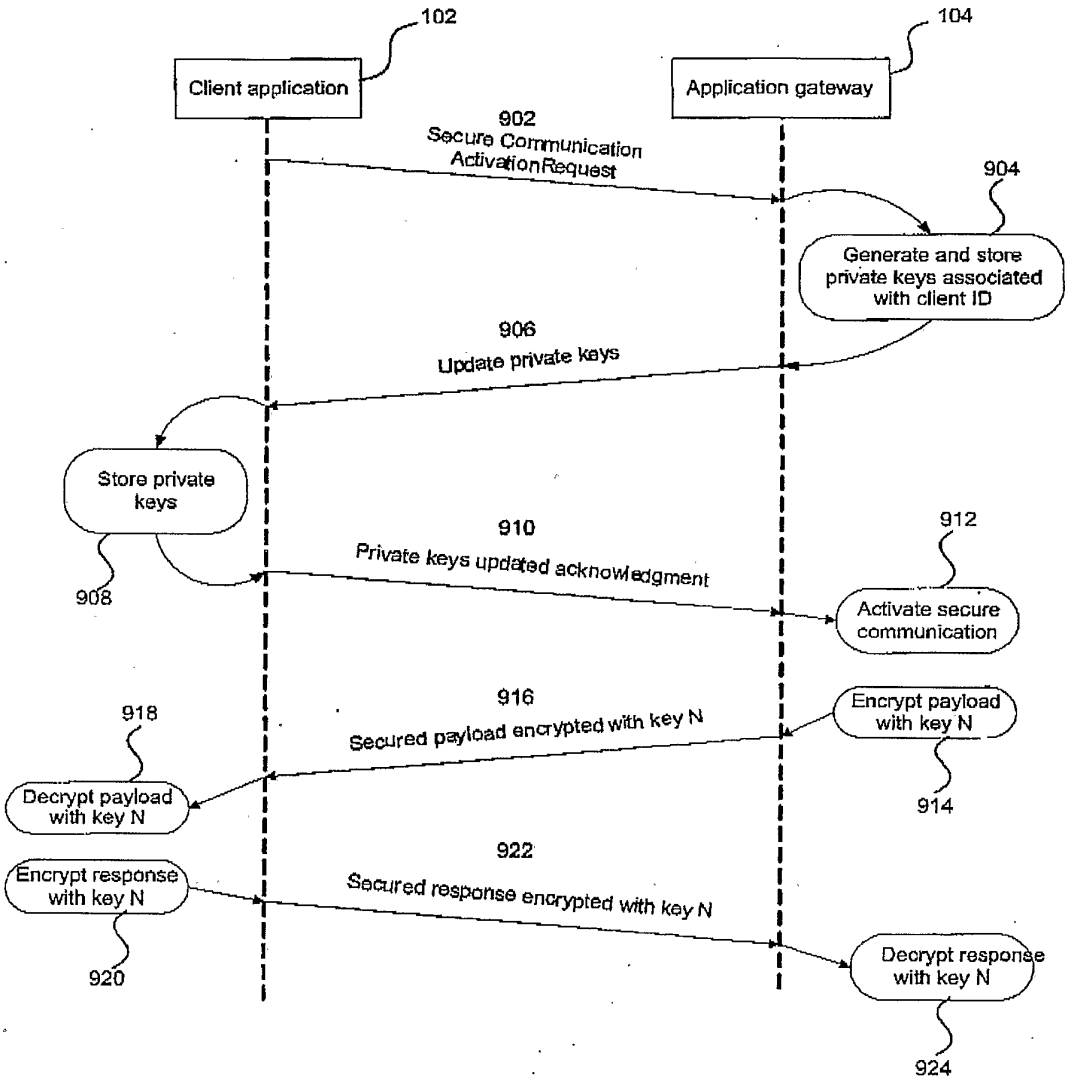

102
Client application
104
Application gateway
902
Secure Communication ActivationRequest
904
Generate and store private keys associated with client ID
906
Update private keys
Store private keys
908
910
Private keys updated acknowledgment
912
Activate secure communication
916
Secured payload encrypted with key N
Encrypt payload with key N
914
918
Decrypt payload with key N
922
Secured response encrypted with key N
Encrypt response with key N
920
Decrypt response with key N
924

FIGURE 10

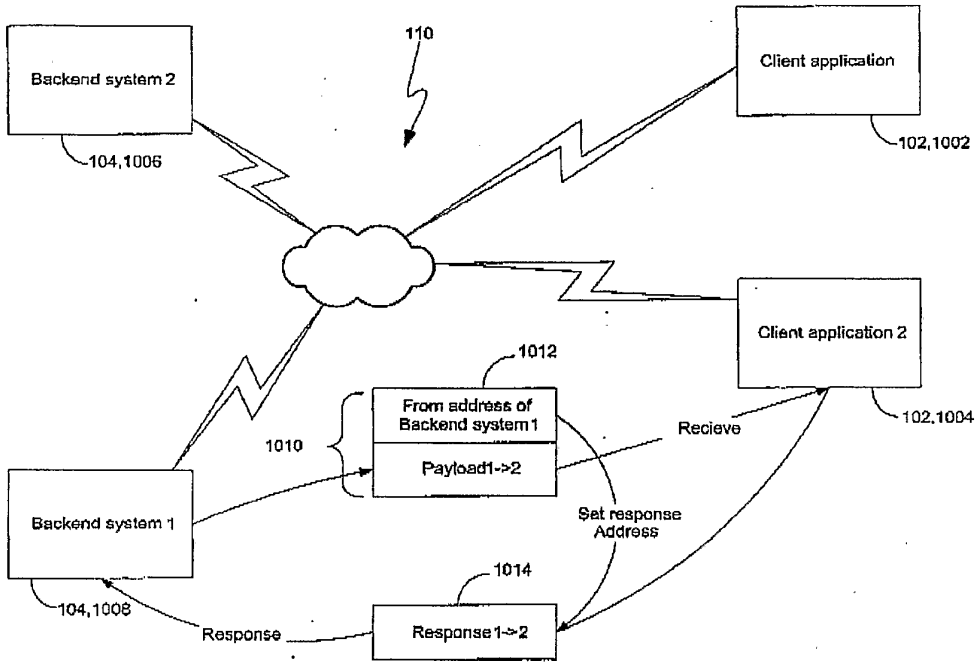

110
Backend system 2
104,1006
Client application
102,1002
Client application 2
102,1004
1012
From address of Backend system 1
Payload1->2
1010
Recieve
Backend system 1
Set response Address
1014
104,1008
Response
Response 1->2

FIGURE 11

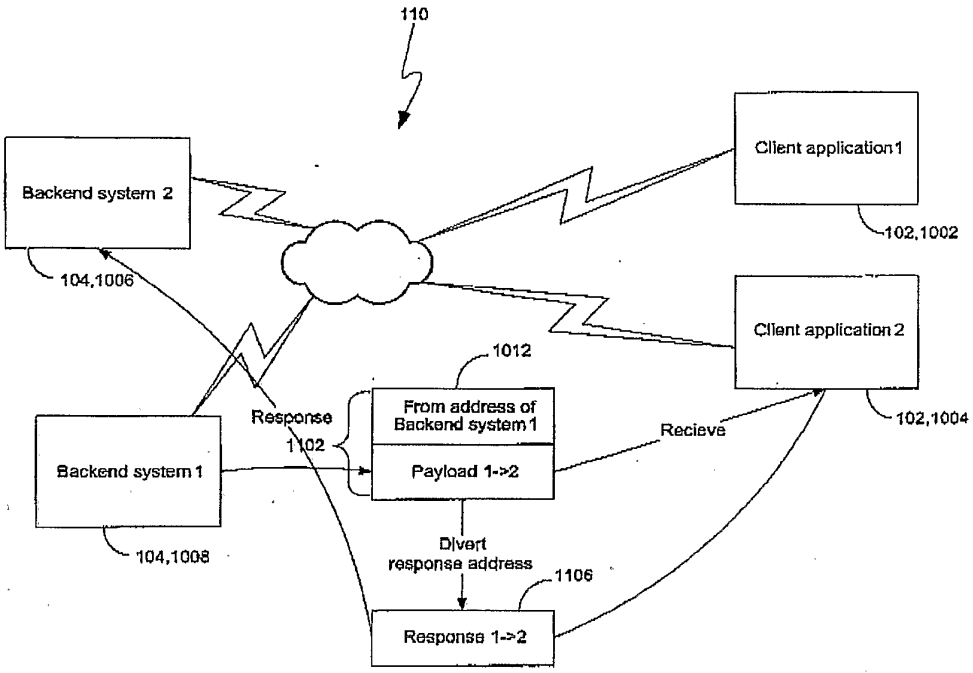

110
Backend system 2
Client application1
102,1002
104,1006
Client application 2
1012
From address of Backend system 1
Response 1102
Recieve
102,1004
Backend system 1
Payload 1->2
104,1008
Divert response address
1106
Response 1->2

FIGURE 12

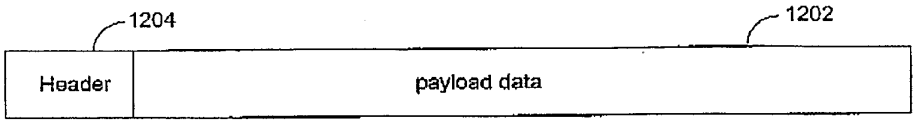


FIGURE 13

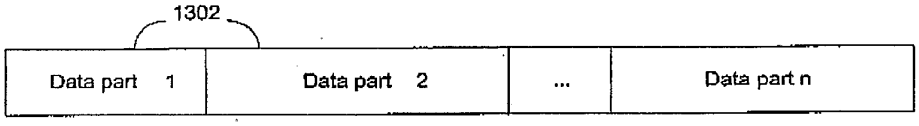


FIGURE 14

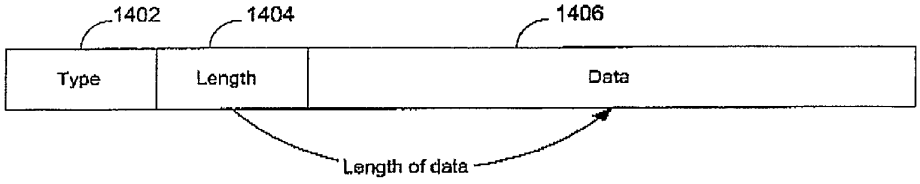


FIGURE 15

Workflow instruction data structure

	Type	Data
Menu Single/Multiple Select	S,M	[PARAMETER] [TITLE] [ITEM1] [ITEM2]..... [ITEMn]
Information Message	I	[TITLE] [MESSAGE]
Header Response	H	[HEADER]
Redirect Address	R	[PHONE NUMBER]
User Input	T	[PARAMETER] [LABEL] [TYPE]
Execute URL	E	[URL]
Jump to index	J	[CMD index]
Go to previous Cmd	P	
Branch menu	B	[PARAMETER] [TITLE] [Label1,index1] [Label2, index2] ..... [ITEMn]
No-op	N	
Store Permanent	K	[Title]
Clear Permanent Storage	D	
Read System Property	P	[Property name]
Configuration Settings	C	[Configurations]

Type enumeration:
TYPE_ANY = 0;
TYPE_EMAILADDR=1;
TYPE_NUMERIC = 2;
TYPE_PHONENUMBER = 3;
TYPE_URL = 4;
TYPE_DECIMAL = 5;

FIGURE 16

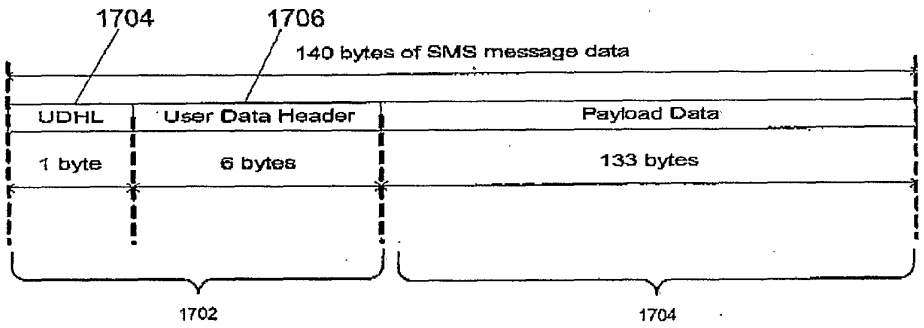

1704
1706
140 bytes of SMS message data
UDHL
User Data Header
Payload Data
1 byte
6 bytes
133 bytes
1702
1704

FIGURE 17

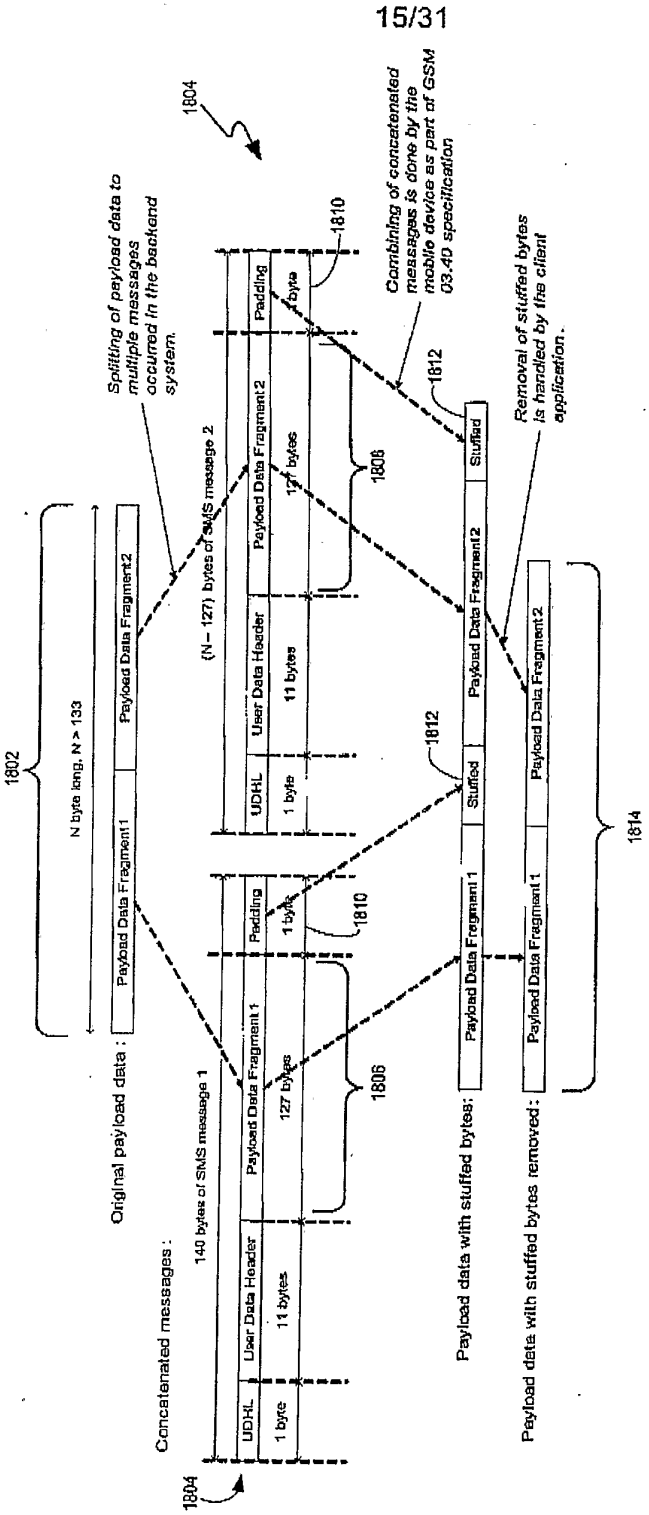

1804
Splitting of payload data to multiple messages occurred in the backend system.
Combining of concatenated messages is done by the mobile device as part of GSM 03.40 specification
Removal of stuffed bytes is handled by the client application.
1802
N byte long, N > 133
Payload Data Fragment1
Payload Data Fragment2
Original payload data :
(N – 127) bytes of SMS message 2
UDHL
User Data Header
Payload Data Fragment2
Padding
1 byte
11 bytes
127 bytes
1 byte
1810
1812
1806
Stuffed
Payload data with stuffed bytes:
Payload data with stuffed bytes removed:
1814
Concatenated messages :
140 bytes of SMS message 1
Payload Data Fragment 1
1804

FIGURE 18

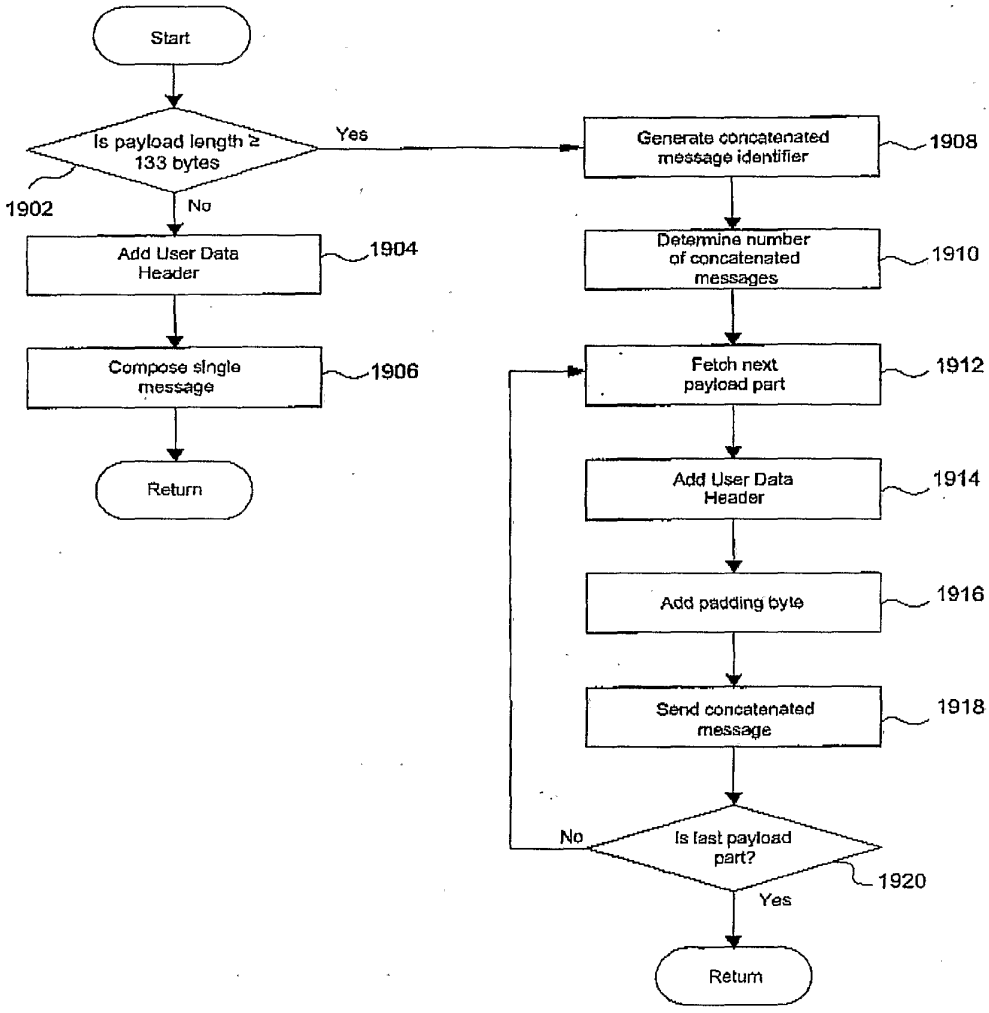

Start
Is payload length ≥ 133 bytes
Yes
No
1902
Add User Data Header
1904
Compose single message
1906
Return
Generate concatenated message identifier
1908
Determine number of concatenated messages
1910
Fetch next payload part
1912
Add User Data Header
1914
Add padding byte
1916
Send concatenated message
1918
Is last payload part?
No
Yes
1920
Return

FIGURE 19

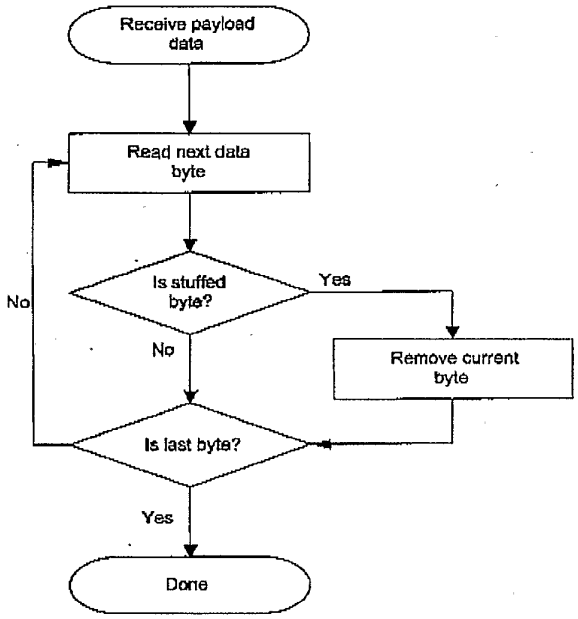

Receive payload data
Read next data byte
Is stuffed byte?
Yes
No
Remove current byte
No
Is last byte?
Yes
Done

FIGURE 20

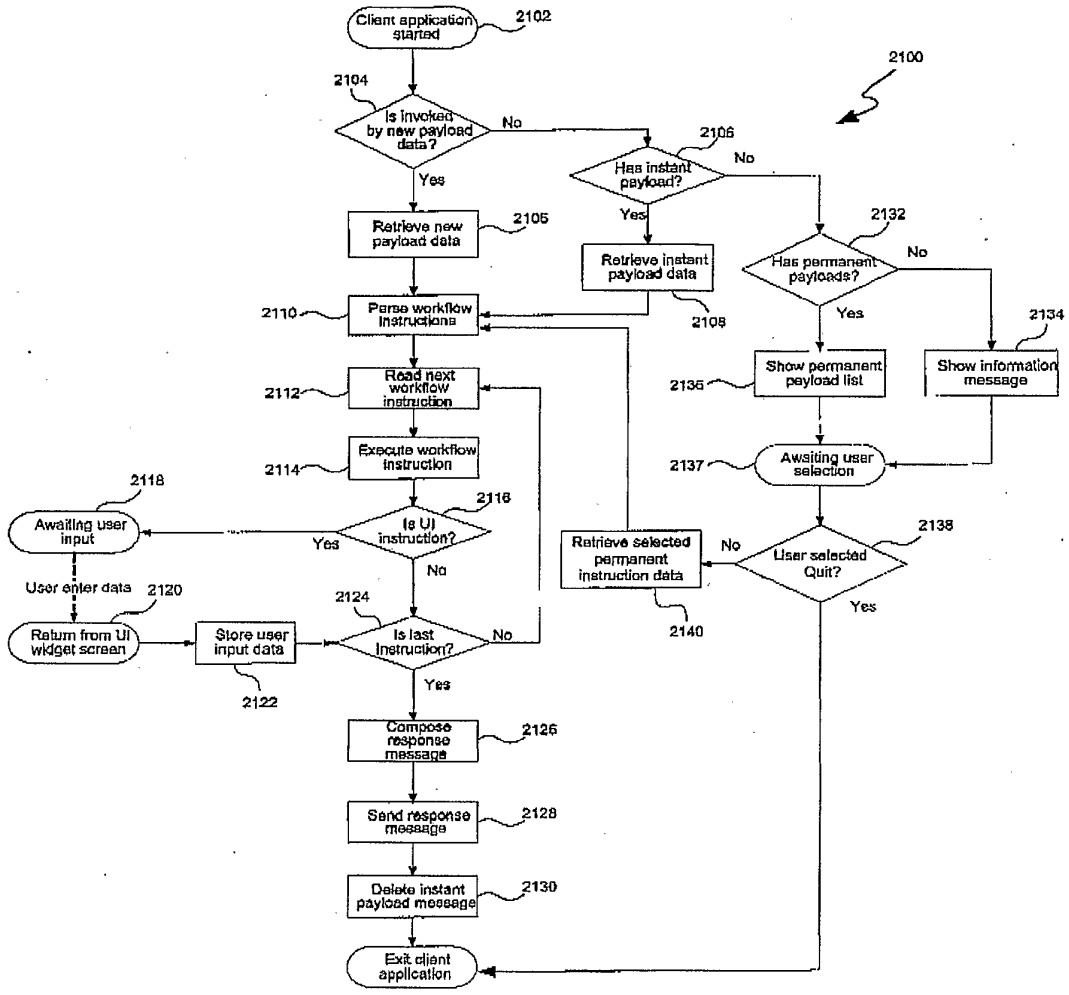

Client application started
2102
2100
2104
Is invoked by new payload data?
No
2106
Has instant payload?
No
Yes
Yes
Retrieve new payload data
2105
Retrieve instant payload data
2108
2132
Has permanent payloads?
No
Yes
2134
2110
Parse workflow instructions
Show permanent payload list
2136
Show information message
2112
Read next workflow instruction
2114
Execute workflow instruction
2137
Awaiting user selection
2118
2116
Awaiting user input
Is UI instruction?
Yes
No
2138
Retrieve selected permanent instruction data
No
User selected Quit?
Yes
2140
User enter data
2120
2124
Return from UI widget screen
Store user input data
Is last Instruction?
No
Yes
2122
Compose response message
2126
Send response message
2128
Delete instant payload message
2130
Exit client application

FIGURE 21

0	Instruction 1 response
1	Instruction 2 response
n	Instruction n response

FIGURE 22

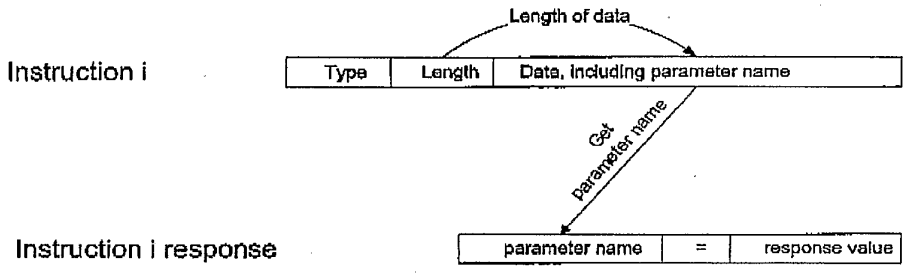


FIGURE 23

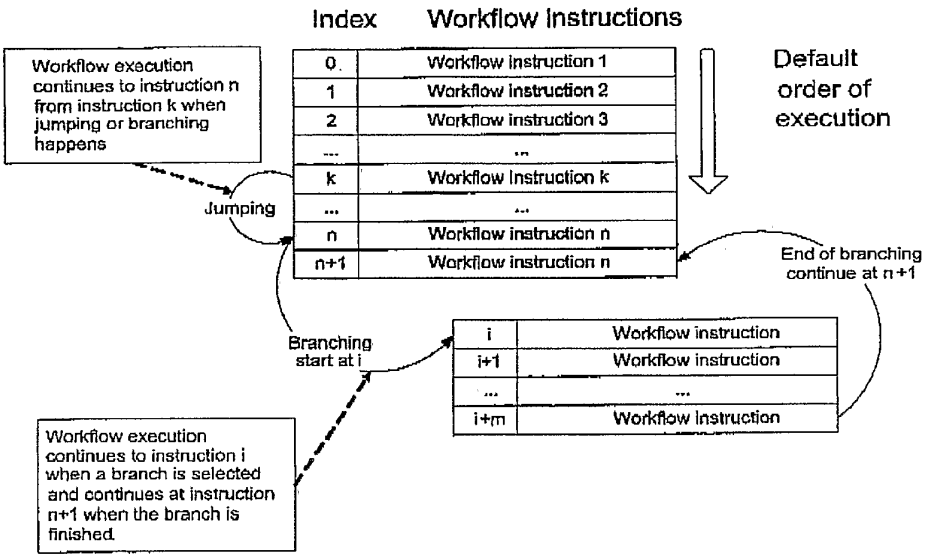

Index
Workflow Instructions
Workflow execution continues to instruction n from instruction k when jumping or branching happens
0
Workflow instruction 1
1
Workflow instruction 2
2
Workflow instruction 3
...
...
k
Workflow instruction k
...
...
n
Workflow instruction n
n+1
Workflow instruction n
Default order of execution
Jumping
End of branching continue at n+1
Branching start at i
i
Workflow instruction
i+1
Workflow instruction
...
...
i+m
Workflow instruction
Workflow execution continues to instruction i when a branch is selected and continues at instruction n+1 when the branch is finished

FIGURE 24

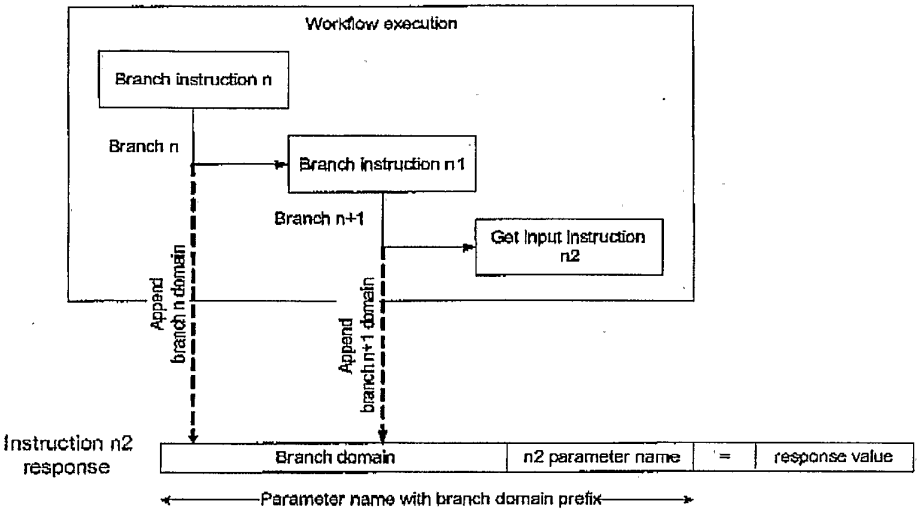

Workflow execution
Branch instruction n
Branch n
Branch instruction n1
Branch n+1
Get Input Instruction n2
Append branch n domain
Append branch n+1 domain
Instruction n2 response
Branch domain
n2 parameter name
=
response value
Parameter name with branch domain prefix

FIGURE 25

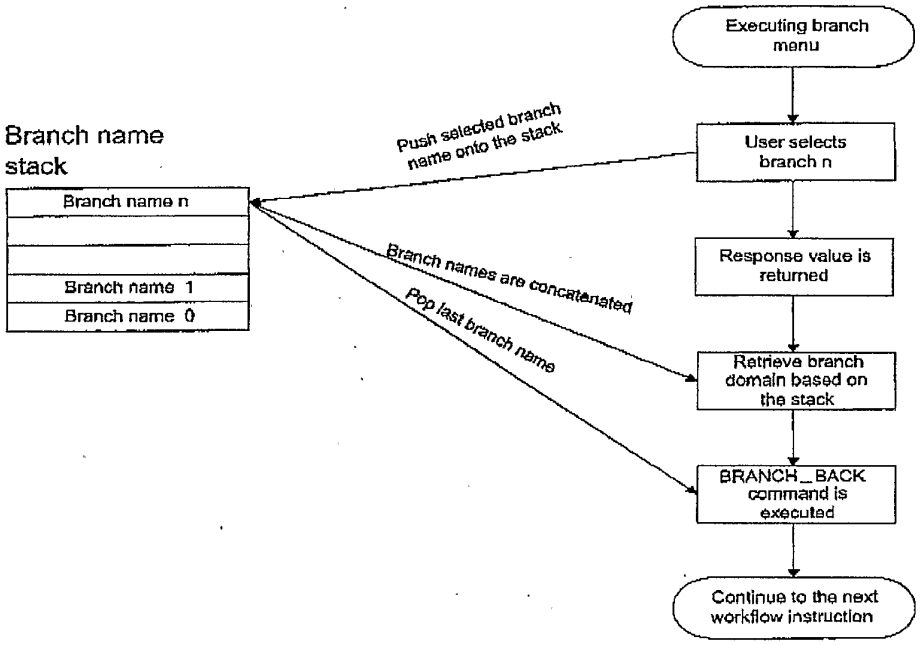

Executing branch menu
User selects branch n
Response value is returned
Retrieve branch domain based on the stack
BRANCH_BACK command is executed
Continue to the next workflow instruction
Push selected branch name onto the stack
Branch names are concatenated
Pop last branch name
Branch name stack
Branch name n
Branch name 1
Branch name 0

FIGURE 26

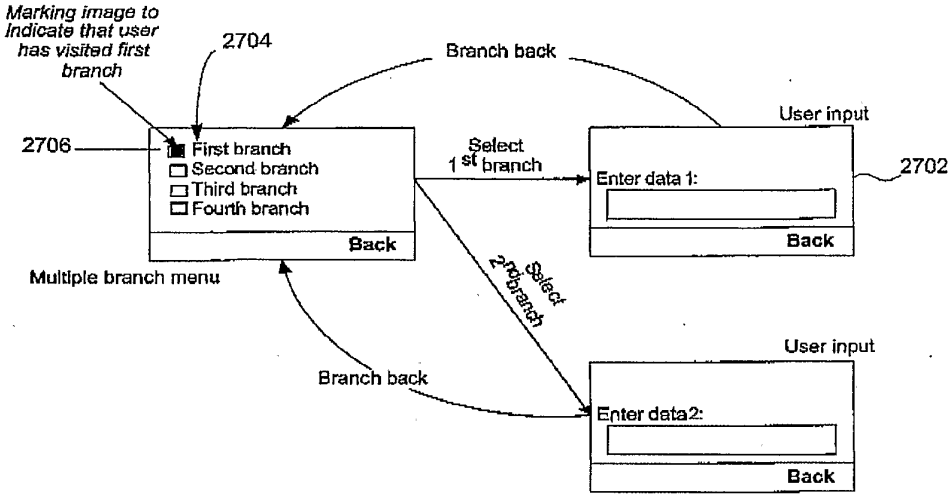


FIGURE 27

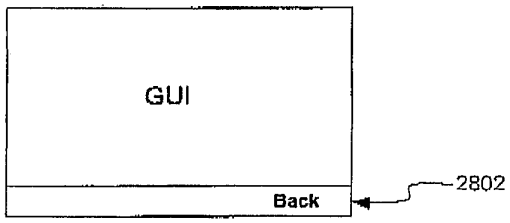


FIGURE 28

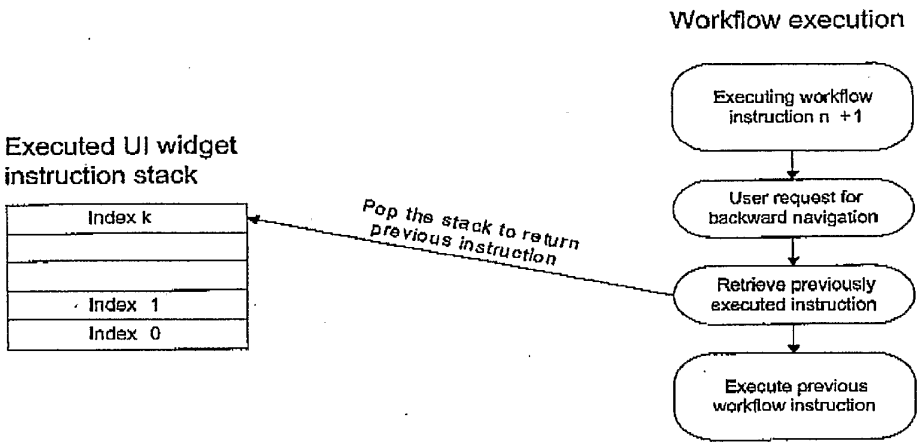

Workflow execution
Executing workflow instruction n +1
User request for backward navigation
Retrieve previously executed instruction
Execute previous workflow instruction
Pop the stack to return previous instruction
Executed UI widget instruction stack
Index k
Index 1
Index 0

FIGURE 29

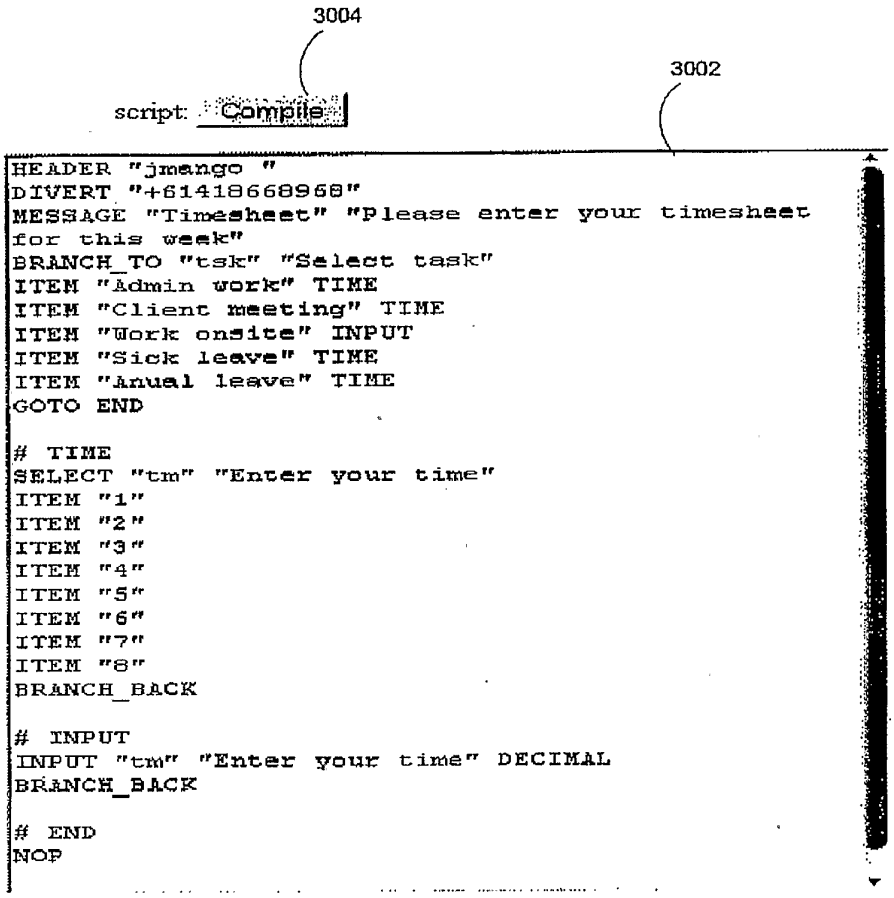

3004
3002
script:
Compile
HEADER "jmango "
DIVERT "+61418668968"
MESSAGE "Timesheet" "Please enter your timesheet
for this week"
BRANCH_TO "tsk" "Select task"
ITEM "Admin work" TIME
ITEM "Client meeting" TIME
ITEM "Work onsite" INPUT
ITEM "Sick leave" TIME
ITEM "Anual leave" TIME
GOTO END
TIME
SELECT "tm" "Enter your time"
ITEM "1"
ITEM "2"
ITEM "3"
ITEM "4"
ITEM "5"
ITEM "6"
ITEM "7"
ITEM "8"
BRANCH_BACK
INPUT
INPUT "tm" "Enter your time" DECIMAL
BRANCH_BACK
END
NOP

FIGURE 30

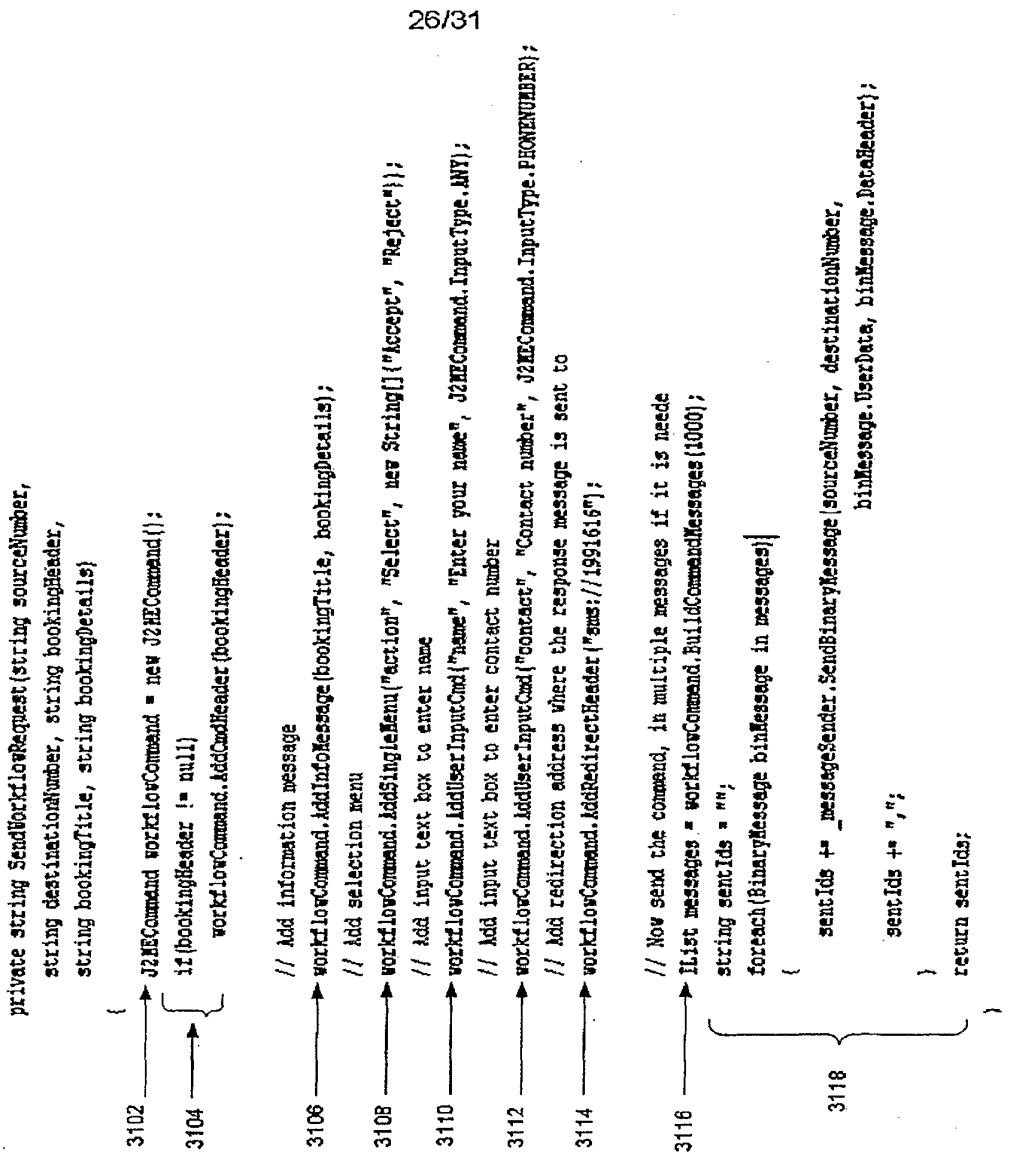

private string SendWorkflowRequest(string sourceNumber,
string destinationNumber, string bookingHeader,
string bookingTitle, string bookingDetails)
{
3102 J2MECommand workflowCommand = new J2MECommand();
3104 if(bookingHeader != null)
workflowCommand.AddCmdHeader(bookingHeader);
// Add information message
3106 workflowCommand.AddInfoMessage(bookingTitle, bookingDetails);
// Add selection menu
3108 workflowCommand.AddSingleMenu("action", "Select", new String[]{"Accept", "Reject"});
// Add input text box to enter name
3110 workflowCommand.AddUserInputCmd("name", "Enter your name", J2MECommand.InputType.ANY);
// Add input text box to enter contact number
3112 workflowCommand.AddUserInputCmd("contact", "Contact number", J2MECommand.InputType.PHONENUMBER);
// Add redirection address where the response message is sent to
3114 workflowCommand.AddRedirectHeader("sms://1991616");
// Now send the command, in multiple messages if it is neede
3116 IList messages = workflowCommand.BuildCommandMessages(1000);
string sentIds = "";
foreach(BinaryMessage binMessage in messages)
{
3118 sentIds += _messageSender.SendBinaryMessage(sourceNumber, destinationNumber,
binMessage.UserData, binMessage.DataHeader);
sentIds += ",";
}
return sentIds;
}

FIGURE 31

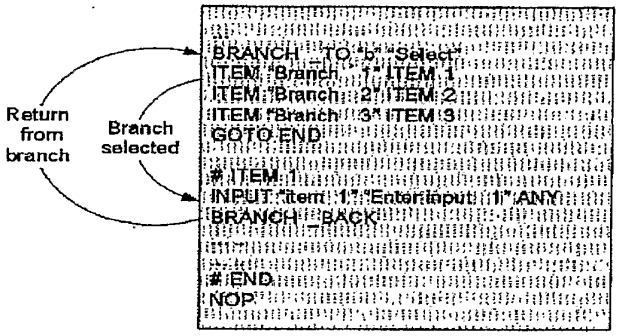


FIGURE 32

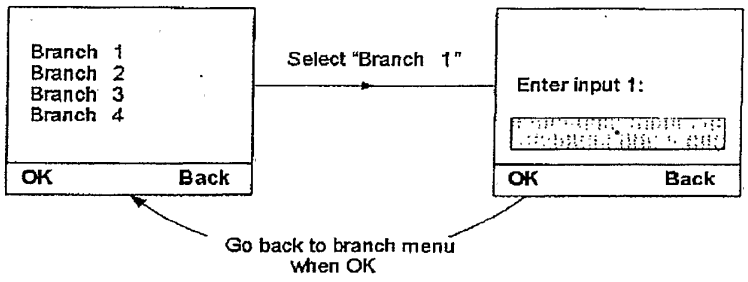


FIGURE 33

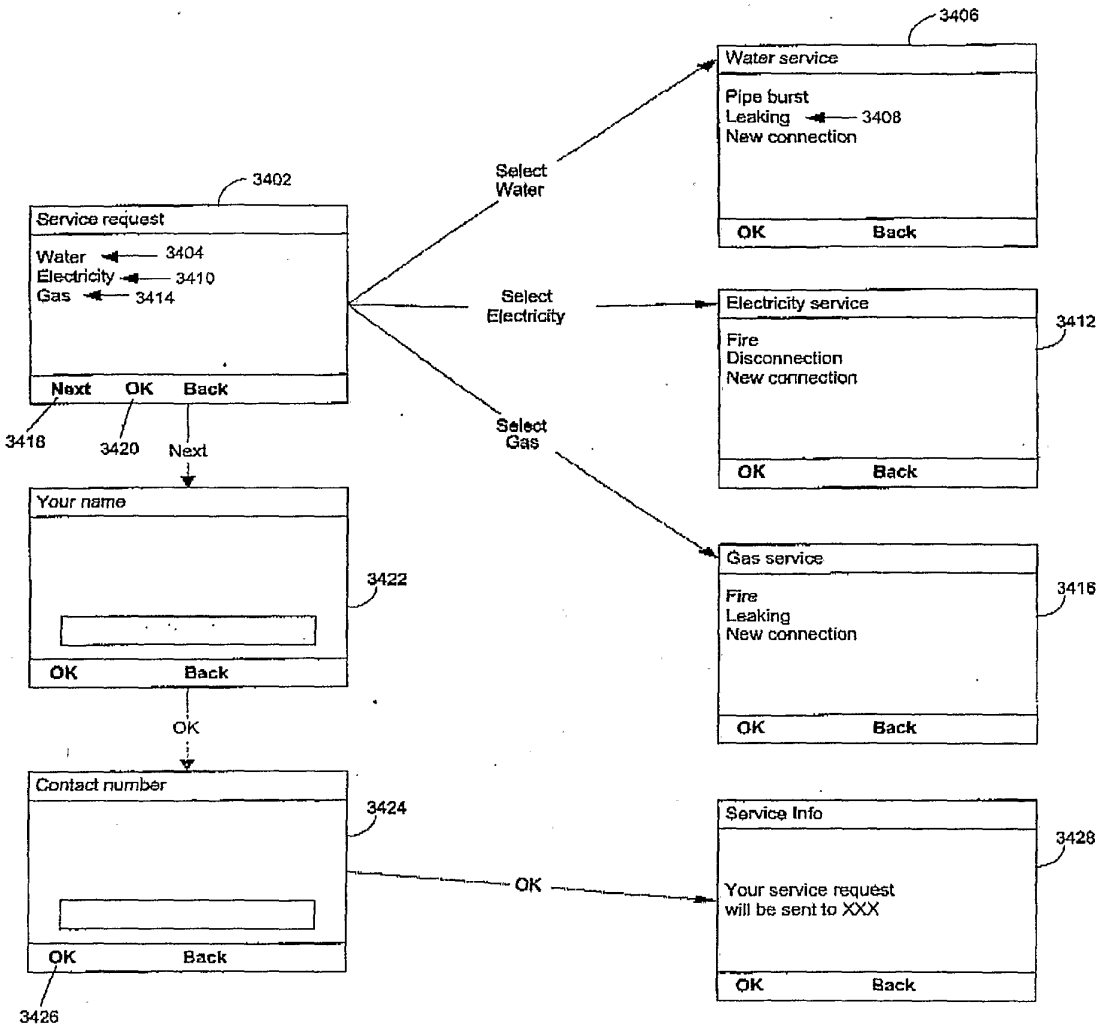

3406
Water service
Pipe burst
Leaking
3408
New connection
OK
Back
3402
Service request
Water
3404
Electricity
3410
Gas
3414
Next
OK
Back
3418
3420
Next
Select Water
Select Electricity
Select Gas
Electricity service
Fire
Disconnection
New connection
OK
Back
3412
Your name
3422
OK
Back
OK
Gas service
Fire
Leaking
New connection
OK
Back
3416
Contact number
3424
OK
Back
3426
OK
Service Info
Your service request will be sent to XXX
OK
Back
3428

FIGURE 34

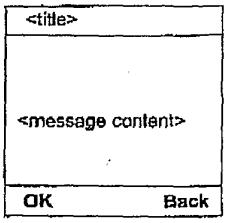


FIGURE 35

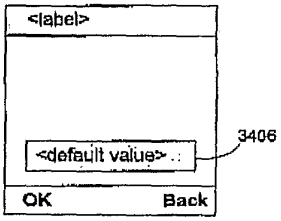


FIGURE 36

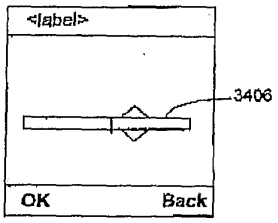


FIGURE 37

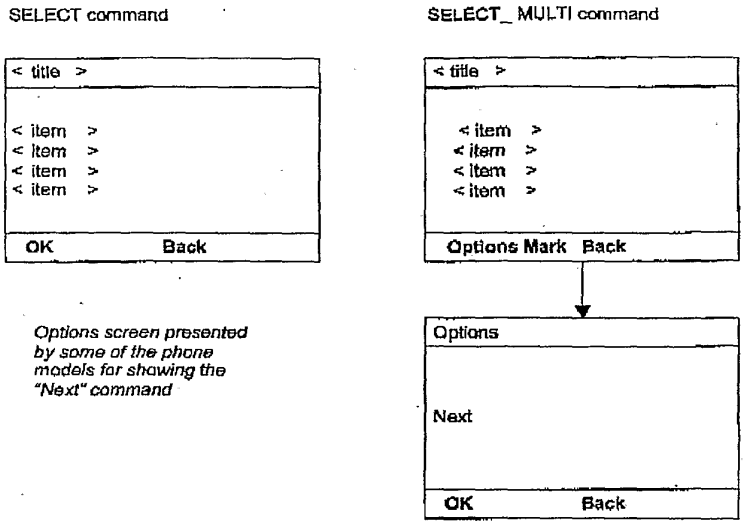

SELECT command
< title >
< item >
< item >
< item >
< item >
OK
Back
Options screen presented by some of the phone models for showing the "Next" command
SELECT_ MULTI command
< title >
< item >
< item >
< item >
< item >
Options Mark Back
Options
Next
OK
Back

FIGURE 38

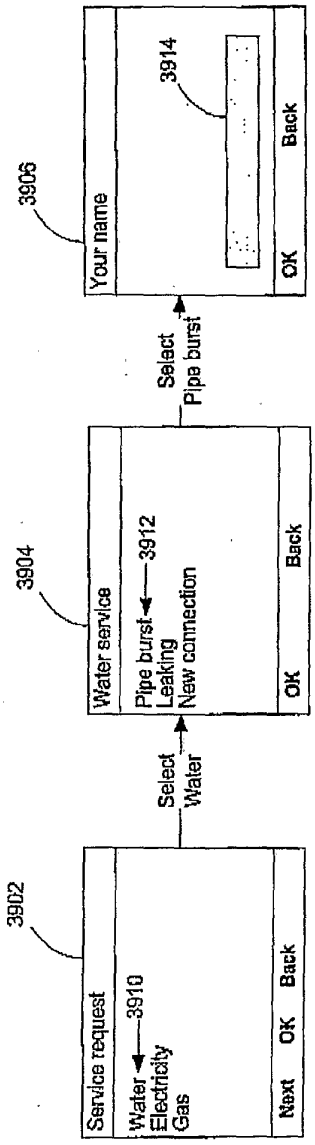

3902
Service request
Water
Electricity
Gas
3910
Next
OK
Back
Select
Water
3904
Water service
Pipe burst
Leaking
New connection
3912
OK
Back
Select
Pipe burst
3906
Your name
3914
OK
Back

FIGURE 39

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001599

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04Q 7/22 (2006.01) ***H04M 3/493*** (2006.01)

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 & USPTO: Keywords: (interactive, SMS, encryption, compile, header, payload and like 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 2006/0095291 A1 (Cherney) 4 May 2006. See for example the title; abstract; fig 4A-4C, 5 and 7; paras [0013]-[0016], [0033]-[0041], [0057]-[0080] and [0089]-[0140].	1-25
X	EP 1509049 A1 (Accenture Global Services GMBH) 20 August 2003. See for example the abstract; paras [0033]-[0039]; and fig 2 and 5.	1-25
A	US 2002/0073023 A1 (Castro et al.) 13 June 2002.	

☐ 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 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
11 December 2007	20 DEC 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Malcolm Peh** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 7914

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2007/001599**

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	2006095291	EP	1836676	US	2006095290	WO	2006050413
EP	1509049	US	2007191032	WO	2005020609		
US	2002073023						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

IP.com Discover Intellectual Property
Search Publish Resources Research and Analytics Blog About Us Contact Us

Electronic settlement system (05-Apr-2002)

Japanese Application Publication (Source: PAJ)
Publication No. JP 2002-99716 A *published on* 05-Apr-2002
Application No. JP 2000-289921 *filed on* 25-Sep-2000

Abstract (English)

PROBLEM TO BE SOLVED: To provide an electronic settlement system capable of preventing a user's privacy from being leaked to outside by preventing a payment code from being used illegally by another person.

SOLUTION: A user connects his/her portable telephone set with a settlement center and inputs the user's ID, password, etc., to request issuing of the payment code. When they are coincident with a user's ID and a password registered in advance, the settlement center issues the payment code. The user notes the payment code. The settlement center gives the information of confirmation to the portable telephone set. The payment code is validated by the user's answering to the information of confirmation. After then, the user does shopping at a store and presents the payment code to the store when paying for it. The store reports the payment code, a charging amount, etc., to the settlement center and after confirmation, the store regard the confirmation as the finish of payment and delivers merchandise. Hereafter, the payment code is invalidated and becomes unusable.

COPYRIGHT: (C)2002,JPO

RECRUIT AGENT
Web・インターネット業界の転職に強い
▶CLICK!

There's no image data available for this publication

Options
More Like This
Download

Inventors
KUNINOBU MASANAO

Applicants
KUNINOBU MASANAO

Classifications
International: **G06F 17/60**

Supplemental Information (Source: DOCDB)

Inventors
KUNINOBU MASANAO

Applicants
KUNINOBU MASANAO

Priority
JP 2000-289921 A 25-Sep-2000

Classifications
International (2006.01): **G06Q 50/00**; G06Q 20/00; G06Q 40/00
International: G06F 17/60

Terms of Use | Privacy Policy | Contact Us
Copyright © 2000-2012 IP.com. All Rights Reserved.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－297198
（P2001－297198A）
(43)公開日　平成13年10月26日(2001.10.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	２５０	Ｇ０６Ｆ　17/60	２５０	３Ｅ０４０
	２３４		２３４Ｚ	５Ｂ０４９
	２３６		２３６Ａ	５Ｂ０５５
	２３８		２３８	５Ｋ０２７
	５０６		５０６	５Ｋ１０１

審査請求　有　　請求項の数８　ＯＬ　（全　６　頁）　最終頁に続く

(21)出願番号　特願2000－113414(P2000－113414)

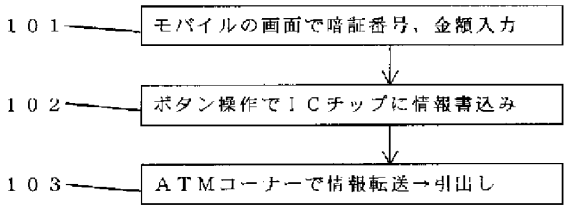
(22)出願日　平成12年４月14日(2000.4.14)

(71)出願人　599175026
株式会社三和銀行
大阪府大阪市中央区伏見町三丁目５番６号
(72)発明者　芦崎　武志
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　三砂　仁
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(74)代理人　100095267
弁理士　小島　高城郎　（外１名）

最終頁に続く

(54)【発明の名称】　携帯電話に組み込まれる金融処理システム

(57)【要約】
【課題】　携帯電話に種々の金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行等を容易に行う。
【解決手段】　携帯電話に組み込まれる金融処理システムにおいて、携帯電話がＩＣチップを内蔵すると共に、ＩＣチップからＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、暗証番号及びＴＭにおける金融処理情報を前記携帯電話に入力した後ＩＣチップに書込み、データ転送手段を介してＩＣチップからＡＴＭへ転送し、ＡＴＭは転送された入力情報に基づいて金融処理を実行する。



1

【特許請求の範囲】

【請求項１】　ＡＴＭにおける金融処理を実行するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、

前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、

前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項２】　前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択されることを特徴とする請求項１に記載の携帯電話に組み込まれる金融処理システム。

【請求項３】　銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、

前記取得したデータを前記表示手段に表示することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項４】　前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含むことを特徴とする請求項３に記載の携帯電話に組み込まれる金融処理システム。

【請求項５】　家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、

家計の収入支出状況に係る情報を前記入力手段により入力し、

前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納することを特徴とする携帯電話に組み込まれる金融処理システム。

【請求項６】　現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、

電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、

前記取得した情報を前記携帯電話へ返送し、

前記返送された情報を前記表示手段により表示することを特徴とする携帯電話に組み込まれるシステム。

2

【請求項７】　前記表示手段による表示に地図が含まれることを特徴とする請求項６に記載の携帯電話に組み込まれるシステム。

【請求項８】　請求項１乃至請求項７のいずれかに記載のシステムを組み込まれたことを特徴とする携帯電話。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話に組み込まれるアプリケーションシステム、特に、金融処理機能及び金融処理に関連する機能を具備するアプリケーションシステムに関する。

【０００２】

【従来の技術】昨今、携帯電話の機能は目覚しく発展しつつあり、インターネットのウェブページの閲覧や電子メールの送受信等、様々な機能が提供されている。その中には、個人の銀行口座の入出金処理いわゆるテレフォンバンキング機能も含まれる。テレフォンバンキングでは、利用者が電話機のプッシュボタンにより暗証番号等を入力した後、入出金処理の種類（振込み、振替等）や金額の入力操作を行うことにより所望する処理が行われる。入力操作に当たっては、自動音声案内または携帯電話の表示画面に表示される指示に従ってプッシュボタンにより適宜の項目を選択する。

【０００３】

【発明が解決しようとする課題】このように、携帯電話における金融処理機能いわゆる金融コンテンツを提供するアプリケーションが種々提供されているが、未だ、口座からの現金の引出し及び口座からの出金による商品代金の決済並びに当該口座の入出金データの整理・保存による家計簿機能等の総合的な個人バンキング処理を実行するアプリケーションは提示されていない。

【０００４】一方、口座からの現金の引出しは、専らＡＴＭを利用して行われることが多いが、キャッシュカードをＡＴＭに挿入してから、暗証番号や引出し金額等の必要な情報をＡＴＭの入力装置に入力しなければならない。現状では、接触型のキャッシュカードが一般的に用いられており、カード挿入及びその後の入力操作に所定の時間が掛かるため、ＡＴＭの混雑時にはいっそうその混雑を増長させることとなる。

【０００５】以上の現状に鑑み、本発明は、携帯電話のアプリケーションとして個人バンキング処理を含めた総合的な機能を具備する金融コンテンツを組込むことにより、携帯電話を利用してＡＴＭからの迅速な現金引出し、各種入出金処理の実行、商品代金の決済、商品受渡し、入出金データの管理を容易に行うことを目的とする。

【０００６】

【課題を解決するための手段】上記の目的を達成するべく、本発明は以下の構成を提供する。

【０００７】（１）ＡＴＭにおける金融処理を実行する

べく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話がＩＣチップを内蔵すると共に、該ＩＣチップから前記ＡＴＭへ非接触にてデータ転送するためのデータ転送手段を設け、前記入力手段を用いて銀行口座に係る暗証番号及び前記ＡＴＭにおける金融処理に係る情報を前記携帯電話に入力した後、該入力した情報を前記ＩＣチップに書込み、前記データ転送手段を介して前記携帯電話の前記ＩＣチップから前記入力情報を前記ＡＴＭへ転送し、前記ＡＴＭは転送された前記入力情報に基づいて前記銀行口座に係る前記金融処理を実行する。

【０００８】（２）上記（１）の構成において、前記金融処理が、残高照会、引出し、入出金明細照会、振込み及び振替を含む群の中から選択される。

【０００９】（３）銀行口座の入出金状況を確認するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、前記携帯電話により前記銀行口座の入出金状況に係る情報を格納したデータベースへ電話回線によりアクセスしデータを取得し、前記取得したデータを前記表示手段に表示する。

【００１０】（４）上記（３）の構成において、前記銀行口座の入出金状況に係る情報が、該銀行口座からの引落しに関する情報であって、引落日、引落内容及び引落金額を含む。

【００１１】（５）家計の収入支出状況を入力するべく入力手段及び表示手段を具備する携帯電話に組み込まれる金融処理システムにおいて、家計の収入支出状況に係る情報を前記入力手段により入力し、前記家計の収入支出状況に係る情報を格納したデータベースへ電話回線によりアクセスすることにより前記入力されたデータを格納する。

【００１２】（６）現在地及び最寄りのＡＴＭ設置場所に関する情報を取得するべく表示手段を具備する携帯電話に組み込まれるシステムにおいて、電話回線により携帯基地局へアクセスし、携帯基地局がＧＰＳを実施することにより前記現在地及び前記最寄りのＡＴＭ設置場所に関する情報を取得し、前記取得した情報を前記携帯電話へ返送し、前記返送された情報を前記表示手段により表示する。

【００１３】（７）上記（６）の構成において、前記表示手段による表示に地図が含まれる。

【００１４】（８）上記（１）乃至上記（７）のいずれかに記載のシステムを組み込まれた携帯電話である。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。本発明における携帯電話（図中では、「モバイル」と称する）は、ＩＣカードに内蔵されると同様のＩＣチップを内蔵し、非接触にてＩＣチップへデータを入出力するために手段を具備する。ＩＣチップは、磁気記録媒体と比べてセキュリティ性が高くかつ大量の情報を記憶できることで知られている。さらに、この携帯電話は、データを入力するためのプッシュボタンまたは類似の入力手段並びにデータを表示するためのディスプレイを具備する。

【００１６】一方、自動取引装置すなわちＡＴＭは、通常、タッチパネルまたはプッシュボタン等のデータの入力手段と表示手段を具備するが、本発明においては特に、非接触にて携帯電話のＩＣチップへデータを書込みまたデータを読取るための手段もまた具備する。

【００１７】斯かる携帯電話の所有者は、ＡＴＭを設置している銀行またはその銀行と提携する銀行に、口座を保有するものとする。当該口座に関連して、口座保有者のみが認知する暗証番号が設定されている。通常、口座保有者はキャッシュカードを所有しており、キャッシュカードをＡＴＭに適用することにより現金の引出しを行うことができる。

【００１８】図１は、本発明による携帯電話における金融処理システムの１つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。ステップ１０１において、口座保有者は、携帯電話の入力手段を用いて暗証番号を入力する。暗証番号は高度の機密事項であるので、入力の際に画面上には暗証番号は明示されず、代わりに「＊」等の記号により入力字数のみが表示される。暗証番号の入力後、口座保有者は、引出し金額を入力する。

【００１９】入力後、ステップ１０２において携帯電話上に設けられた所定のボタンを押すことにより、あるいは他の適宜の操作により、携帯電話に内蔵されたＩＣチップに入力された情報を書込む。

【００２０】ステップ１０１及び１０２は、ＡＴＭ設置場所へ赴く前に予め行っておくことが好ましい。本発明の利点の１つは、ＡＴＭ設置場所以外の任意の場所で、予め現金引出しのための必要な操作を行うことができることである。

【００２１】ステップ１０３において、口座保有者はＡＴＭに赴き、携帯電話のＩＣチップ内の情報をＡＴＭの読取り手段に読取らせることにより、ＩＣチップ内の情報を転送する。これは、非接触にて行われる。ＡＴＭからオンラインにてホストコンピュータへの照会が実行され、暗証番号により本人確認できたならば、ＡＴＭから入力情報で指定された金額の現金が出金される。

【００２２】図２は、携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である。先ず、初期画面においては、携帯電話に組み込まれる金融コンテンツの一覧が示される。例えば、残高照会、引出し、入出金明細照会、振込み、振替、マネーカレンダーである。マネーカレンダーについては後述する。ここでは「２．引出し」を選択するとする。すると、次画面で、暗証番号と引出し金額の入力が促される。

【００２３】図３は、図２の初期画面において「４．振込み」を選択する場合の表示例を示した図である。次画面において、本人確認のための暗証番号、振込み金額及び振込先を入力する。さらに、振込み操作においては、振込み相手に対するメッセージを添付することができる。メッセージを添付したい場合は、メッセージ内容及び相手のメールアドレスを入力する。これらの入力を終えたならば、入力情報をＩＣチップに書込む。その後、ＡＴＭにおいて入力情報をＡＴＭに読取らせると、直ちに振込みが実行される。メッセージがある場合は、相手にメッセージが送られる。この振込み機能により、ショッピングが可能となる。例えば、商品販売する店舗の口座へ振込みを行うと共に、所望する商品内容をメッセージにて店舗に伝えることにより、商品代金の決済が完了し、後日商品が届けられることとなる。

【００２４】図４は、図２の初期画面において「６．マネーカレンダー」を選択する場合の表示例を示した図である。「マネーカレンダー」においては、銀行口座の入出金状況の確認及び家計の収入支出に関する情報の入出力を行う。図４では、マネーカレンダーの項目として、引落日情報及び家計簿入力が挙げられている。「１．引落日情報」を選択した場合、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスすることにより、近日中に口座引落しされる項目の情報を取得し、それが表示される。情報には、引落しの日付、内容及び金額が示されている。これにより口座保有者は、必要な口座残高を確保するよう注意することができる。

【００２５】マネーカレンダーの「２．家計簿入力」を選択した場合は、家計簿へ記録すべき内容すなわち家計における収入支出状況を入力することができる。図５は、家計簿入力を選択した場合の表示例を示した図である。入力は、画面に表示された指示に沿って行えば容易に行える。先ず、利用金額を入力し、次に利用用途を複数の項目から選択することにより入力すると、確認画面が表示される。確認画面では、入力内容がまとめて示され、間違いなければ、「２．追加入力」を選択することにより、電話回線を通して銀行のホストコンピュータの管理するデータベースへアクセスし、入力データが送られ、データベースに入力データが格納される。家計簿情報は、入力を修正する場合は、「ＰＤＡで編集」を選択することにより編集する。尚、ショッピング内容を家計簿入力する場合、店舗のＰＯＳと携帯電話が互いに通信し、店舗のＰＯＳから入力データが転送されることにより、自動入力してもよい。

【００２６】本発明に係る携帯電話は、好適にはＪＡＶＡ言語を搭載しており、入力操作及びメモ・編集操作を効率的に行うことができる。

【００２７】種々の金融コンテンツからなる金融処理システムを組み込んだ本発明の携帯電話は、近年、コンビニエンスストアに設置されるようになったＡＴＭや２４時間営業ＡＴＭにおいて利用する場合に特に有用である。場所や時間を限定されること無く、いつでも容易にバンキング処理が可能となるからである。

【００２８】従って、図６に示すＡＴＭ設置場所情報提供機能を付加することにより、本発明に係る携帯電話は、さらに効果的に利用されることとなる。図６は、ＡＴＭの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す。ディスプレイ上には、現在地の周辺地図が表示されると共に、最も近い２４時間営業の銀行ＡＴＭ、及び、ＡＴＭ設置コンビニエンスストアが表示されている。具体的な実施方法としては、携帯電話の基地局を活用してＧＰＳ（広域位置情報機能）サービスを実施する。携帯電話はＪＡＶＡ言語を搭載しており、先ず、利用者が携帯電話を用いて基地局のホストへアクセスする。基地局のホストは、ＧＰＳを実施することにより携帯電話の現在位置情報を取得し、最寄りのキャッシュポイントすなわちＡＴＭ設置場所の情報を地図及びテキストデータで携帯電話へ返送する。利用者はディスプレイに表示された地図を見て最寄りのＡＴＭを知ることができる。

【００２９】

【発明の効果】本発明においては、携帯電話自体がＩＣチップを搭載し、ＩＣチップに書込んだ情報を非接触にてＡＴＭに読取らせることができる。従って、携帯電話をキャッシュカードの代わり用いてＡＴＭ操作することができる。携帯電話のＩＣチップには、予め必要な入力情報を書込んでおくことができるため、ＡＴＭ設置場所においては、現金引出しや振込み等の処理を容易にかつ速やかに行うことができる。よってＡＴＭの混雑緩和に多大に寄与することとなる。

【００３０】振込み機能にはメッセージ添付機能があり、オンラインショッピングの代金決済が可能であると同時に、商品の受渡しに関する情報をメッセージで伝えることができる。

【００３１】また、携帯電話により、銀行口座の入出金及び家計の収入支出に関する情報の入力及び出力を行うことができるため、いつでも、どこでも簡単に日々のお金の利用状況を確認したり編集したりすることが可能となる。家計簿を継続的につけることは面倒であり長続きしないことが多いが、本発明のシステムを用いれば、クレジットカード等の引落日を確認しながら、無駄なく上手にお金を消費することができる。

【００３２】さらに、携帯電話を通して２４時間営業のＡＴＭや、ＡＴＭを設置したコンビニエンスストアの位置情報を得られるため、携帯電話に組み込まれた金融コンテンツを利用できる場所へ利用者を用意に導くことができ、極めて利便性の高いしシステムが実現される。

【図面の簡単な説明】

【図１】本発明による携帯電話における金融処理システ

ムの１つである現金引出し機能を利用する場合の操作フローを示す概略的な流れ図である。

【図２】携帯電話での現金引出し操作における携帯電話のディスプレイ上の表示例を示した図である。

【図３】図２の初期画面において「４．振込み」を選択する場合の表示例を示した図である。

【図４】図２の初期画面において「６．マネーカレンダー」を選択する場合の表示例を示した図である。

【図５】図４の次画面において「２．家計簿入力」を選択した場合の表示例を示した図である。

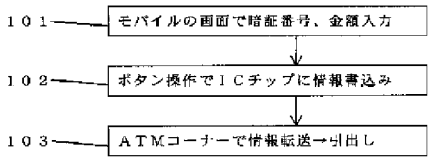
【図６】ＡＴＭの設置場所情報を提供する機能を具備する携帯電話のディスプレイ表示例を示す図である。

【符号の説明】

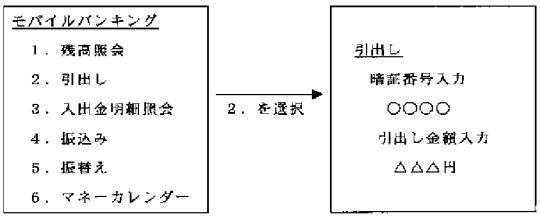
１０　携帯電話

１２　ディスプレイ

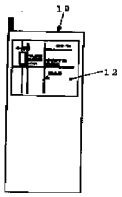
【図１】



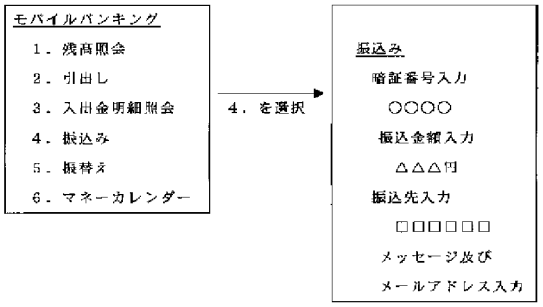
【図２】



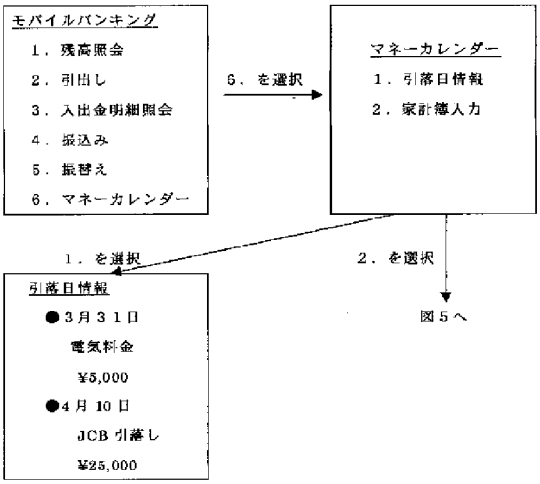
【図６】



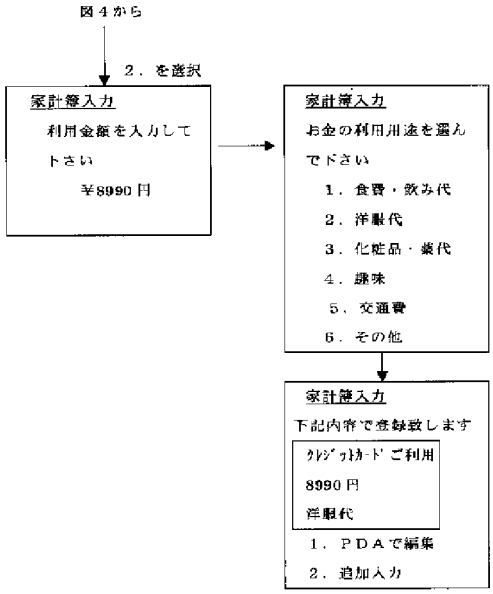
【図３】



【図４】



【図５】



フロントページの続き

(51)Int.Cl.[7]		識別記号	F I		テーマコード（参考）
Ｇ０７Ｄ	9/00	４５１	Ｇ０７Ｄ　9/00	４５１Ｃ	９Ａ００１
Ｇ０７Ｆ	19/00		Ｈ０４Ｍ　1/00	Ｒ	
Ｈ０４Ｍ	1/00		1/725		
	1/725		11/00	３０３	
	11/00	３０３	Ｇ０７Ｄ　9/00	４７６	

(72)発明者　中村　喜治
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　山本　泰三
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内
(72)発明者　森田　直樹
東京都千代田区大手町１丁目１番１号　株式会社三和銀行内

Ｆターム(参考)　3E040 BA07 BA18 CA14 EA01 EA02 FH05
5B049 AA02 BB46 CC36 GG06
5B055 BB03 CB01 CB08 CB09 PA05 PA11
5K027 AA11 FF01 FF22
5K101 KK11 KK15 LL12 NN01 NN18
9A001 JJ64 KK56 KK58

DERWENT-ACC-NO: 2002-023233

DERWENT-WEEK: 200203

COPYRIGHT 2012 DERWENT INFORMATION LTD

TITLE: Financial processing system in mobile telephones, has integrated circuit chip built in telephone, which stores input financial process information including bank account number which is then transmitted to ATM

INVENTOR: ASHIZAKI T; MISAGO H ; MORITA N ; NAKAMURA Y ; YAMAMOTO T

PATENT-ASSIGNEE: MIWA GINKO KK[MIWAN]

PRIORITY-DATA: 2000JP-113414 (April 14, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
JP 2001297198 A	October 26, 2001	JA

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP2001297198A	N/A	2000JP-113414	April 14, 2000

INT-CL-CURRENT:

TYPE	IPC DATE
CIPP	G07D9/00 20060101
CIPS	G06Q10/00 20060101
CIPS	G06Q40/00 20060101
CIPS	G07F19/00 20060101
CIPS	H04M1/00 20060101
CIPS	H04M1/725 20060101
CIPS	H04M11/00 20060101

ABSTRACTED-PUB-NO: JP 2001297198 A

BASIC-ABSTRACT:

NOVELTY - The financial process information input as a code number along with the bank account number is written in an integrated circuit (IC) chip built in a telephone. A data transmitter transmits the data from the IC chip to an automatic teller machine (ATM) which executes the financial process based on the transferred information.

USE - Is built in the mobile telephone for financial processing in banks.

ADVANTAGE - Performs quick and easy execution of various deposit and withdrawal processes, etc.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram of operation of financial processing system. (Drawing includes non-English language text).

CHOSEN-DRAWING: Dwg.1/6

TITLE-TERMS: FINANCIAL PROCESS SYSTEM MOBILE TELEPHONE INTEGRATE CIRCUIT CHIP BUILD STORAGE INPUT INFORMATION BANK ACCOUNT NUMBER TRANSMIT ATM

DERWENT-CLASS: T01 T05 W01

EPI-CODES: T01-J05A; T05-L; T05-L03; W01-C01; W01-C01D1; W01-C05;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2002-018604

Espacenet

Bibliographic data: JP2001357164 (A) — 2001-12-26

METHOD AND CENTER FOR FUND MANAGEMENT

Inventor(s): SAKAMOTO HIROAKI; TAKAHASHI YOSHIO; TABUCHI EIJI; OGURO HIROAKI; HANIYUDA HIRONORI; HASEGAWA TAKESHI; IIJIMA MIKIMASA; SUDO MASANORI ± (SAKAMOTO HIROAKI, ; TAKAHASHI YOSHIO, ; TABUCHI EIJI, ; OGURO HIROAKI, ; HANIYUDA HIRONORI, ; HASEGAWA TAKESHI, ; IIJIMA MIKIMASA, ; SUDO MASANORI)

Applicant(s): NTT DATA CORP ± (NTT DATA CORP)

Classification: - **international:** ***G06Q50/00; G07C13/00;*** (IPC1-7): G06F17/60; G07C13/00

- **Euro:**

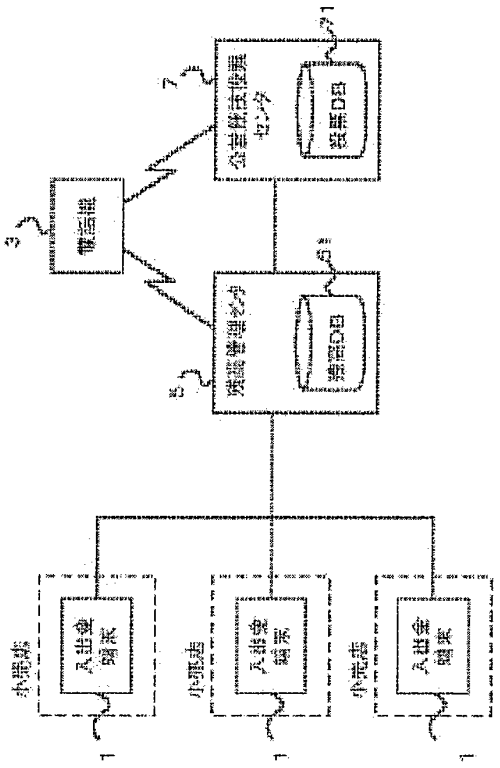
Application number: JP20000178134 20000614

Priority number(s): JP20000178134 20000614

Abstract of JP2001357164 (A)

PROBLEM TO BE SOLVED: To provide a method and a center for fund management which is convenient for a betting system. SOLUTION: A balance management center 5 having a balance database 51 which stores balance data consisting of a telephone number for authentication, the balance, and a password code for each user adds a paid-back amount to the balance of the balance data of a winner according to winning data received from a municipally operated race betting center 7 and pays winning money back. Further, the balance management center 5 answers a payment request from a telephone set 3, specifies balance data corresponding to a specified telephone number for authentication in the balance database 51, and updates the balance according to an withdrawal amount and supplies a withdrawal reception number to the user after authenticating the user. The balance management center 5, after verifying the withdrawal reception number on a reception number verification request from a money paying and receiving terminal 1, allows money to be paid. In response, the store where the money paying and receiving terminal 1 is installed supplies the cash corresponding to the withdrawal amount to the user.

Last updated: 24.09.2012 Worldwide
Database 5.7.44.2; 93p



APPL-1002
APPLE INC. / Page 520 of 1892

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020020065989 A**

(21)Application number: **1020010006133**

(22)Date of filing: **08.02.2001**

(30)Priority: ..

(51)Int. Cl **G06F 17/60**

(71)Applicant: **STARBRIDGE COMMUNICATIONS CO., LTD.**

(72)Inventor: **CHOI, JONG HO**

(54) **PAYMENT METHOD USING PAYMENT CODE ON MOBILE TERMINAL**

(57) Abstract:

PURPOSE: A payment method is provided to make a payment on a mobile terminal by using an identifiable payment code downloaded at a mobile terminal via an online network or an offline media or given at every transaction. CONSTITUTION: The method comprises steps of a user requesting a payment on a mobile phone(S101), a mobile payment management company setting a monthly payment limit to the user by considering a vocation, an age or an income, and transmitting a payment code to the user(S102), the user downloading the payment code at the mobile phone(S103), in a case of buying a commodity or using a service by using a mobile payment, the user inputting a secret code at the mobile terminal for receiving a user approval(S104), the mobile phone displaying the payment code on a display(S105), a payment code reader, installed at an affiliated store, reading the payment code displayed on the mobile phone(S106), the payment code reader allowing an operator to input a transaction money or an installment month as well as the payment code, and transmitting a transaction approval request to the mobile payment management company(S107), the company transmitting a transaction approval code and specification to the reader and the mobile phone after checking if the requested transaction is normal(S110), and a mobile communication company calculating a total payment amount and sending a bill to the user(S111).

copyright KIPO 2003

Legal Status

Date of request for an examination (20010208)

Notification date of refusal decision ( )

Final disposal of an application (rejection)
Date of final disposal of an application (20031209)
Patent registration number ( )
Date of registration ( )
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020030068603 A**

(21)Application number: **1020020008052**

(22)Date of filing: **15.02.2002**

(30)Priority: ..

(51)Int. Cl **G06F 17/60**

(71)Applicant: **NARU SYSTEM CO., LTD.**

(72)Inventor: **KIM, GYEONG SIK**

(54) **SYSTEM AND METHOD FOR SETTLING CHARGE USING CELLULAR PHONE**

(57) Abstract:

PURPOSE: A system and a method for settling charge using a cellular phone are provided to realize a micro remittance function and an accumulation function as well as a micro payment function by using the cellular phone of the wireless communication without the wired Internet environment. CONSTITUTION: A user section(52) is a buyer checking processor generated when a buyer starts transaction. An input server(54) stores a transaction request as a queue format. A customer information confirmation part(56) verifies a cellular phone number of the buyer and a seller by linking with a mobile communication companys data part(58). A mobile account(62) is a virtual account linked with a real account of a bank or a credit card company(64). A limit/remainder confirmation part (60) decides the transaction by checking the remainder or a credit limit of the mobile account(62). A certification number generating part(66) generates a number for the identification and the approval of the transaction. A transaction particulars server(68) changes the virtual account of the buyer and the seller after confirming the transaction particulars and the certification number from the buyer.

copyright KIPO 2003

Legal Status

Date of request for an examination (20020219)

Notification date of refusal decision (00000000)

Final disposal of an application (rejection)

Date of final disposal of an application (20040213)

Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020070092400 A**

(21)Application number: **1020060022464**
(22)Date of filing: **10.03.2006**
(30)Priority: ..
(51)Int. Cl **G06Q 20/00**

(71)Applicant: **SHIN HAN BANK**
(72)Inventor: **JUNG, JONG PIL**
KIM, KI JUNG

(54) **SYSTEM AND A METHOD FOR PROVIDING A CONVENIENT/SAFE ONE-STOP NON-FACIAL CHANNEL PAYMENT SERVICE BY USING A NICKNAME**



(57) Abstract:

PURPOSE: A system and a method for processing payment by using a nickname are provided to offer an one-stop non-facial channel payment service for online non-facial channel payment by replacing a payment account number for a non-facial channel with the nickname. CONSTITUTION: An information inputting part(115) receives nickname information set to a virtual account connected to a real account of a customer. An information storing part(120) stores the nickname to a storage medium(130) by linking with virtual/real account and customer information. An interface provider(110) transmits a payment form or window to a customer terminal when the customer performs the payment in the online network. A payment processor receives mobile number/nickname information from the customer terminal and transmits an authentication code to the mobile terminal by using the mobile number. If the authentication code is received from the customer terminal, the payment processor authenticates the customer and processes an approval for the payment by checking the virtual account.

copyright KIPO 2007

Legal Status
Date of request for an examination (20060310)
Notification date of refusal decision (00000000)
Final disposal of an application (registration)
Date of final disposal of an application (20080319)

Patent registration number (1008229850000)
Date of registration (20080410)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2001 (27.09.2001)

PCT

(10) International Publication Number
WO 01/71627 A2

(51) International Patent Classification[7]: G06F 17/60, G07F 7/10, H04L 29/06

(21) International Application Number: PCT/US01/09136

(22) International Filing Date: 21 March 2001 (21.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/532,507 22 March 2000 (22.03.2000) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventor: **BLOW, Anthony, Talmage**; 5511 Las Alturas Terrace, San Diego, CA 92114 (US).

(74) Agents: **WADSWORTH, Philip, R.** et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

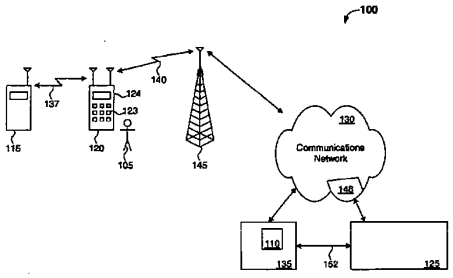
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD,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

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

(54) Title: A METHOD AND SYSTEM FOR WIRELESS ELECTRONIC COMMERCE USING A PORTABLE, WIRELESS COMMUNICATION DEVICE HAVING UNIQUE IDENTIFYING INFORMATION



(57) Abstract: A method and system for effecting an electronic commerce (e-commerce) transaction, wherein a mobile subscriber/user initiates and controls the transaction at or near a local point-of-transaction (POT) terminal using a portable Wireless Communication Device (WCD). An e-commerce support provider (ESP) computer connected with the Internet participates in and facilitates the e-commerce transaction. Using the WCD, the user electronically transfers user owned assets, such as money, credit, or bonus points, held in a remote consumer asset account, from the asset account to the POT terminal as payment for goods and/or services at the POT. The WCD is uniquely identified by unique identifying information stored in the WCD. The WCD includes a first wireless interface for communicating with a wireless interface in the local POT terminal. First e-commerce transaction data is transmitted between the WCD and the POT terminal using the first wireless interface. The WCD includes a second wireless interface for communicating with the ESP computer. Encrypted second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data is transmitted between the WCD and the ESP computer connected with the Internet, using the second wireless interface of the WCD. The exchange of first and second e-commerce transaction data between the POT terminal, the WCD, and the ESP computer, results in the transfer of user assets between the POT terminal and the WCD necessary to effect the e-commerce transaction.

WO 01/71627 A2

A METHOD AND SYSTEM FOR WIRELESS ELECTRONIC COMMERCE USING A PORTABLE, WIRELESS COMMUNICATION DEVICE HAVING UNIQUE IDENTIFYING INFORMATION

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to electronic commerce, and more particularly, to effecting a wireless electronic commerce transaction using a wireless communication device.

Related Art

Many commerce transactions require a consumer to be physically at or near a point-of-sale or point-of-transaction (POT) where the consumer exchanges money, or a money substitute, to pay for goods and/or services. Such transactions include, for example, purchasing goods or merchandise at a grocery or department store cash register, buying a meal at a restaurant, depositing money in a parking meter, and a cash exchange between two co-located individuals. In these transactions, a typically mobile consumer uses cash, a credit card, or a check as a medium of exchange or payment directly at the POT. Such forms of payment have certain disadvantages. For example, the cash, check and credit card are easily lost. The credit card, when lost, and even when not lost, is a frequent target of fraudulent use by unscrupulous individuals. Also, point-of-sale paper work involved with the credit card and check, and the additional personal identification (usually a driver's license) required to consummate a check transaction, can be a hassle.

Nowadays, the Internet provides a consumer with a rich medium for electronic commerce (herein referred to as e-commerce). A powerful Internet infrastructure, including a plethora of Internet service and support providers, provides the consumer with many beneficial services related to electronic commerce transactions. For example, a consumer can conveniently "shop" in the privacy of his or her own home using a relatively cheap personal computer connected with the Internet. Typically, the consumer purchases goods and/or service from a remote or distant e-commerce shopping partner, also connected with the Internet, by authorizing a credit payment to the shopping partner. Such e-commerce transactions are disadvantageously limited to the extent that the e-commerce shopping partner must be Internet accessible. In other words, the transaction requires a network connection between both partners in the transaction.

Hence, there is a need to effect a commerce transaction in such a way as to overcome the above mentioned disadvantages.

There is a further need to provide security in a commerce transaction to thereby protect the privacy of the transaction and the consumer effecting the transaction.

There is an even further need to effect an electronic commerce transaction between first and second partners and using a network such as the Internet, wherein only one of the partners requires network access.

There is a need to effect an electronic commerce transaction using the Internet, wherein a mobile consumer can be at or near a point-of-transaction, as required, to pay for goods and/or services or to receive payment from the point-of-transaction.

SUMMARY OF THE INVENTION

The present invention provides a method and system for effecting an e-commerce transaction, wherein a mobile subscriber/user initiates and controls the transaction at or near a local POT terminal using a portable Wireless Communication Device (WCD). An e-commerce support provider (ESP) computer connected with the Internet participates in and facilitates the e-commerce transaction. Using the WCD, the user electronically transfers user owned assets, such as money, credit, or bonus points, held in a remote consumer asset account, from the asset account to the POT terminal as payment for goods and/or services at the POT.

The WCD is uniquely identified by unique identifying information stored in the WCD. The WCD includes a first wireless interface for communicating with a wireless interface in the local POT terminal. First e-commerce transaction data is transmitted between the WCD and the POT terminal using the first wireless interface. The WCD includes a second wireless interface for communicating with the ESP computer. Encrypted second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data is transmitted between the WCD and the ESP computer connected with the Internet, using the second wireless interface of the WCD. The exchange of first and second e-commerce transaction data between the POT terminal, the WCD, and the ESP computer, results in the transfer of user assets between the POT terminal and the WCD necessary to effect the e-commerce transaction.

Features and advantages

The present invention advantageously preserves the mobility of a consumer in an e-commerce transaction, whereby the consumer can participate in the e-commerce transaction at or near a POT. The present invention permits the consumer to initiate and control an electronic transfer of consumer owned assets, such as money, to pay for goods and services at the POT. The present invention thereby avoids the need for and pitfalls associated with using conventional mediums of exchange, such as cash, a credit card, or a check.

The present invention advantageously provides Internet connectivity and support to a mobile user in an e-commerce transaction while adding a level of security and privacy to the transaction. Also, a POT terminal in accordance with the present need not be Internet accessible to participate in the e-commerce transaction.

The WCD of the present invention serves as a kind of "electronic wallet" that is convenient to carry, and private and secure in use.

BRIEF DESCRIPTION OF THE FIGURES

The foregoing and other features and advantages of the invention will be apparent from the following, more particular description of a preferred embodiment of the invention, as illustrated in the accompanying drawings.

FIG. 1 is an overview of a system for effecting an e-commerce transaction in accordance with the present invention

FIG. 2A is an illustration of exemplary memory buffer in the WCD of FIG. 1.

FIG. 2B is an exemplary format of an encrypted e-commerce transaction digital data packet exchanged between a WCD and an ESP computer of FIG. 1.

FIG. 2C is an exemplary format of an e-commerce transaction digital data packet exchanged between a WCD and a POT terminal of FIG. 1.

FIG. 3 is a block diagram of an embodiment of a logical architecture corresponding to the system of FIG. 1.

FIG. 4 is an e-commerce transaction process of corresponding to an e-commerce transaction in the system of FIG. 1.

FIG. 5 is an illustration of an encryption/decryption function of FIG. 3.

FIG. 6 is a block diagram of an arrangement for an electronic transfer of assets from a WCD to another WCD.

FIG. 7 is a block diagram of an arrangement for effecting an e-commerce transaction using a WCD capable of scanning merchandise bar codes.

FIG. 8 is a block diagram of an embodiment of the WCD of FIG. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 1 is an overview of a system 100 for effecting an e-commerce transaction in accordance with the present invention. In system 100, a subscriber/user 105 owns assets held in an asset account 110. User 105 initiates and controls an electronic transfer of assets between the asset account 110 and a POT terminal 115 using a portable WCD 120. Portable WCD 120 includes an input device 123 and a display device 124 enabling user 105 to participate in the e-commerce transaction via the WCD. In an example transaction where asset account 110 is a user bank

account, user 105 uses system 100 to electronically transfer money from his or her bank account 110 to POT terminal 115 to purchase goods or services at the POT terminal. In an alternative arrangement, the user electronically transfers assets in an opposite direction, that is, from POT terminal 115 to his or her bank account 110. In the e-commerce transaction of the present invention, POT terminal 115 and WCD 120 are relatively nearby or local to one another while asset account 110 is relatively distant or remote from both POT terminal 115 and WCD 120.

To facilitate the above mentioned electronic transfer of assets, system 100 includes an ESP computer 125 linked with a communication network 130. ESP computer 125, which can reside in an Internet support provider facility, preferably provides centralized, Internet processing support in many e-commerce transactions of the present invention. In the embodiment of FIG. 1, ESP computer 125 communicates with both WCD 120 and an e-commerce facility135, such as a bank, holding asset account 110, such that asset account is electronically accessible to ESP computer 125.

WCD 120 includes a first wireless interface for wirelessly communicating with a compatible wireless interface in POT terminal 115 over a short-range wireless communications link137. WCD 120 exchanges e-commerce transaction messages in the form of digital data packets with POT terminal 115 over short-range wireless communications link 137. WCD 120 also includes a second wireless interface for wirelessly communicating with ESP computer 125. WCD 120 is uniquely identified by unique identifying information stored in WCD 120, and also available to ESP computer 125. To maintain a required level of security and privacy in the e-commerce transaction, WCD 120 and ESP computer 125 exchange encrypted e-commerce transaction

messages, also in the form of digital data packets, generated as a function of the unique identifying information.

Since WCD 120 communicates wirelessly with both POT terminal 115 and ESP computer 125, system 100 advantageously permits user mobility in any e-commerce transaction of the present invention. Thus, portable WCD 120 conveniently functions as a kind of "electronic wallet" or "pocket book" because user 105 carries WCD 120 to the POT (that is, near to POT terminal 115) and uses WCD 120 as the conduit for a secure and private electronic transfer of money or other asset to or from POT terminal 115. Another advantage of the present invention is that POT terminal 115 can be a stand-alone electronic device, since POT terminal 115 need not be network accessible.

WCD 120 and ESP computer 125 communicate via 1) a wireless communication link 140 between the WCD and a communication network access device 145, such as a radio base station or the like, and 2) communication network 130. Communication network 130 encompasses the world wide packet data communications network commonly referred to as the Internet, local area networks, and the public switched telephone network. ESP computer 125 can be connected to the Internet via, for example, an Internet service provider 148. An Internet address corresponding to ESP computer 125 is stored in the memory of WCD 120, and an Internet address corresponding to WCD 120 is stored in a memory of ESP computer 125. This enables WCD 120 and ESP computer 125 to establish Internet connections between each other for the exchange of encrypted data packets during an e-commerce transaction.

As previously mentioned, ESP computer 125 also communicates with e-commerce facility 135, such as a bank, wherein asset account 110 is typically held. ESP computer 125 and e-commerce facility 135 communicate with each other via

communication network 130 and/or a dedicated communication link 152. In an alternative arrangement of system 100, asset account 110 is co-located with ESP computer 125, thus obviating the need for additional communications between ESP computer 125 and e-commerce facility 135.

In the present invention, WCD 120 and ESP computer 125 both include memory for storing the unique identification information associated with WCD 120. Such identification information includes an Electronic Serial Number (ESN), a Mobile Subscriber Number (MSN), and a user/subscriber access Personal Identification Number (PIN) or password. The ESN uniquely identifies WCD 120 and is programmed into the memory device of WCD 120 at a factory where WCD 120 is manufactured. The MSN also uniquely identifies WCD 120 and can serve as a network address of WCD 120. The user selects the PIN and enters the PIN into the memory buffer of WCD 120 using input device 123. The PIN thus serves as a password required for using WCD 120. WCD 120 and ESP computer 125 use the unique identification information to establish a network connection between each other, to uniquely identify each e-commerce transaction, and to generate the encrypted e-commerce transaction data packets.

An exemplary memory buffer 200 of WCD 120 for storing the unique identifying information of the WCD, is depicted in FIG. 2A. Memory buffer 200 includes memory locations 202, 204, 206 and 208 for respectively storing an ESN, an MSN, a PIN and an Internet address for ESP computer 125. A similar memory buffer resides in ESP computer 125, except that the memory buffer of ESP computer 125 includes an Internet address for WCD 120.

FIG. 2B is an exemplary format of an encrypted e-commerce transaction digital data packet 220 exchanged between WCD 120 and ESP computer 125. Packet 220 includes a message

type field 222, a WCD address field 224, and an encrypted data payload 226. Message type field 222 contains a message type specifier indicating a message type, such as a request, response or any other message type. WCD address field 224 includes a network address, such as an MSN (for example, the MSN of WCD 120), corresponding to the WCD that is either the originator or destination of the message in data packet 220. Data payload 226 includes the encrypted content of a message. Packet 220 also includes any additional fields required to support a particular application or communication protocol, such as an Internet communication protocol (IP). In the preferred embodiment, data packet 220 is further formatted in accordance with Internet communication protocols, such as an Internet Point-to-Point protocol (PPP) and TCP/IP.

FIG. 2C is an exemplary format of an e-commerce transaction digital data packet 230 exchanged between WCD 120 and POT terminal 115, over wireless link 137. Data packet 230 includes a header field 235 containing any header information required to support a particular application. Packet 230 also includes a data payload 240 containing the content of a message. The content of the message can be formatted as a simple ASCII character string, in the HyperText Markup Language (HTML), in the Wireless Markup Language (WML)(also known as the Hand held Devices Markup Language (HDML)), or in accordance with any other format, so long as a message received by WCD 120 can be displayed to user 105 by WCD 120, when necessary, and as described below.

FIG. 3 is an embodiment of a logical architecture corresponding to system 100. POT terminal 115, WCD 120 and ESP computer 125 each include memory and computer processing capability sufficient to host and execute software programs or applications required to support an e-commerce transaction.

WCD 120 hosts an e-commerce client application 300, including for example, a known browser application, and an e-commerce server application 325. ESP computer 125 hosts an ESP application 330, including new transaction, billing/accounting, and communication software applications. Also, WCD 120 and ESP computer 125 host complementary encryption/decryption functions 335 and 340, respectively, for generating the encrypted e-commerce transaction data packets mentioned in connection with FIG. 1, and for decrypting these encrypted packets. POT terminal 115 hosts an e-commerce application server 345 and is capable of electronically receiving assets, such as money, as payment for goods and/or services.

E-commerce client 300 of WDC 120 transmits request messages to and receives response messages from ESP application 330. E-commerce client application 300 also includes a user control interface for respectively displaying messages to and receiving e-commerce transaction control commands from user display device 124 and user input device 123 of WCD 120, thus allowing user 105 to participate in and control the e-commerce transaction. E-commerce client 300 transmits request messages to and receives response messages from e-commerce application server 345 in POT terminal 115. Messages received by e-commerce client application 300 can be displayed to the user device as and when appropriate. For example, an HTML or HDML command sequence transmitted by POT terminal 115 can be displayed by client 300, as is done with known browser applications.

An e-commerce transaction process of the present invention is depicted in FIG. 4. FIG. 4 corresponds to an e-commerce transaction in the system of FIG. 1. The process begins at a step 402 when user 105 initiates the e-commerce transaction using WCD 120, for example, by pressing a start key or the like on

the WCD. At a step 405, WCD 120 transmits a request message to POT terminal 115 requesting POT terminal specific e-commerce information from the POT terminal. At a step 410, POT terminal 115 transmits a response message including the specific e-commerce information to WCD 120. At a step 415, WCD 120 receives the response message. WCD 120 displays necessary information relating to and/or received from POT terminal 115 to user 105 and prompts the user for input if necessary. WCD 120 accepts information and/or commands entered by user 105 via input device 123 of WCD 120.

At a step 420, WCD 120 generates an encrypted request message based on or as a function of some or all of the information and/or commands received from POT terminal 115 and user 105, and using the unique identification information associated with the WCD. A typical encrypted request message, in accordance with the format of message 220, includes a "request" message type specifier in message type field 222, the MSN of WCD 120 in address field 224, and an encrypted message as payload 226. One or more of the MSN, ESN and PIN of WCD 120 are used to generate encrypted payload 226. WCD 120 transmits the encrypted request message to ESP computer 125.

At a step 425, ESP computer 125 receives the encrypted request message, verifies the address in field 224, and decrypts the encrypted message using the same unique identification information, for example the ESN, MSN, and/or PIN, as was used to encrypt the message in step 420. Next, at a step 427, ESP computer 125 establishes communications with remote e-commerce facility 135 to verify/validate the e-commerce transaction in real-time, that is, right away, and in relation to user asset account 110 held at the e-commerce facility. For example, ESP computer 125 validates the e-commerce transaction by

verifying there are sufficient assets in asset account 110 to satisfy an asset amount requested in the request message from WCD 120.

In one exemplary verification/validation process, ESP computer 125 transmits the MSN (and PIN if required) to e-commerce facility 135. In turn, e-commerce facility 135 identifies user asset account 110 using the MSN (and PIN if required). This being done, ESP computer 125 solicits an "approval" from e-commerce facility 135 indicating there are sufficient funds available in asset account 110 to satisfy or "cover" an asset amount requested in the request message from WCD 120, that is necessary to complete the e-commerce transaction at the POT terminal.

At a step 430, ESP computer 125 generates an encrypted verification/validation response message using the same unique identification information as was used in step 420, and transmits the message to WCD 120. The response message indicates whether the e-commerce transaction is approved. At a step 435, after receiving the verification/validation response message, WCD 120 transmits a message including required assets to POT terminal 115 if the received verification/validation response message indicates an approved or validated e-commerce transaction. At a step 440, after further communication between ESP computer 125 and facility 135, asset account 110 is debited to reflect the consummated e-commerce transaction, that is, the electronic transfer of user owned assets from asset account 110 to POT terminal 115.

With regard to the user PIN, different levels of security are advantageously provided in the present invention. For example, WCD 120 can provide the user with a menu of security options. Such options, when selected, can require the user to enter the PIN 1) before every e-commerce transaction, 2) periodically, for example, every X hours (where X is 1, 2 etc.), 3) upon powering on WCD, or 4) when the e-commerce transaction involves at least a

predetermined amount of assets or money. Such security features decrease the chances of any fraudulent use of WCD 120 in an e-commerce transaction.

FIG. 5 is an illustration of encryption/decryption function 335 of FIG. 3. Encryption/decryption functions 335 and 340 are the same, and therefor, a description of one suffices for the other. Encryption/decryption function 335 includes an encryption sub-function 500 for encrypting transaction data 505 with unique identification information 510, to generate encrypted e-commerce transaction data 515. Encryption sub-function 500 uses any known encryption algorithm providing the level of security and privacy required for the e-commerce transaction, so long as the unique identification information of WCD 120 can be used to encrypt the transaction data 505. Exemplary encryption/decryption protocols useable in the present invention include, but are not limited to, the Data Encryption Standard (DES) encryption protocol, and the Pretty Good Privacy (PGP) protocol commonly used to encrypt electronic mail and Internet files.

Encrypted data 515 generated by encryption sub-function 500 represents payload 226 of message 220. Transaction data 505 is based on information received from POT terminal 115 and user input at WCD 120. Unique identification information 510 includes at least one of the MSN, ESN and PIN associated with WCD 125. Encryption/decryption function 335 also includes a decryption sub-function 520 for decrypting encrypted transaction data 525 with unique identification information 510, to generate decrypted e-commerce transaction data 530.

In the following exemplary "parking meter" e-commerce transaction, POT terminal 115 is a parking meter capable of accepting electronic money deposits transmitted to the meter by WCD 120. User 105 initiates the parking meter e-commerce

transaction by depressing the start key of WCD 120 when the user (carrying WCD 120) is within a wireless communication range of parking meter 115. In response, WCD 120 requests parking meter specific information from parking meter 115. Parking meter 115 responds with an exemplary message:

METER202398981:

THIS METER COSTS $0.25 an hour, PAY?

This message, once received by WCD 120, is displayed to user 105 via the WCD display device. User 105 responds by depressing a WCD key indicating "YES ", the user wishes to pay for an hour of parking. In response to the "YES" key being depressed, WCD 120 transmits an encrypted request to ESP 125 for approval to transfer $0.25 from user bank account 110 to the parking meter. Assuming a bank account balance of greater than $0.25 in bank account 110, bank facility 135 approves the transfer, and in turn, ESP 125 transmits an encrypted approval message to WCD 120. After receiving the approval message, WCD 120 transmits a message including a $0.25 monetary transfer to parking meter 115 to complete the transaction and to pay for one hour of parking. After the transaction is complete, ESP 125 reestablishes communication with facility 135 to thereby debit bank account 110 by $.25.

In the following exemplary "restaurant-based" e-commerce transaction, POT terminal 115 resides in a restaurant and stores restaurant specific information such as a food and beverage menu with associated prices. In this example, user 105 again initiates the e-commerce transaction by depressing the start key of WCD 120 when in communication range of POT terminal 115. In response to the request transmitted by WCD 120, restaurant POT terminal 115 transmits a response message to the WCD 120. The response message includes the food and beverage menu and associated prices. This information is displayed to user 105 at

WCD 120. User 105 selects desired items from the displayed menu via input device 123 of WCD 120. WCD 120 automatically calculates a total cost of the selected items (including a designated tip if the user so desires), and transmits an encrypted message to ESP computer 125 for approval of this total cost amount. If ESP computer 120 approves the transaction, WCD 120 transmits an electronic payment to POT terminal 115 at the restaurant.

The e-commerce transactions described above each involve an electronic transfer of assets, such as money, from WCD 120 to POT terminal 115 at the POT. However, it should be appreciated that POT terminal 115 can be a second WCD, whereby assets are transferred electronically from WCD 120 to the second WCD. FIG. 6 is a block diagram of an arrangement 600 for such an electronic transfer of assets from WCD 120 to a WCD 605. Arrangement 600 is similar to the arrangement described in connection with system 100, except WCD 605 replaces POT terminal 115. Arrangement 600 also includes ESP computer 610 and an e-commerce facility 612, for supporting an e-commerce transaction effected using WCD 605. A user 615 owns assets in an asset account 620 held by e-commerce facility 612. WCD 605, ESP 610 and e-commerce facility 612 inter-communicate in the same manner that WCD 120, ESP 125, and e-commerce facility 135 inter-communicate.

In arrangement 600, user 615 can initiate and control an electronic transfer of assets from asset account 620 to asset account 110 using WCD 605. An exemplary transfer, wherein asset accounts 620 and 110 are bank accounts, includes the electronic transfer of money from bank account 620 to bank account 110, as now described. When user 615 initiates such a transaction at WCD 605, WCD 605 transmits an initial request to WCD 120. In response, e-commerce server application 325 of WCD 120 (see FIG. 3) generates a response message identifying WCD 120. Next,

at WCD 605, user 615 enters a dollar amount that is to be transferred from account 620 to account 110. Next a transfer of this amount is verified/validated by ESP 610 and e-commerce facility 612 in the same manner as described above in connection with FIG. 4. After such validation, WCD 605 transmits a message to WCD 120 electronically transferring the entered dollar amount to WCD 120. Finally, the account balances of asset accounts 620 and 110 are respectively debited and credited by the dollar amount transferred between the accounts to reflect the e-commerce transaction.

FIG. 7 is a block diagram of another arrangement 700 of the present invention for effecting an e-commerce transaction using a WCD 705 capable of scanning a merchandise bar code associated with a merchandise item 710. WCD 705 is interconnected with an ESP computer and bank facility as described above, but not shown in FIG. 7. The first wireless interface of WCD 705, that is, the short range wireless interface, includes a known bar code reader 715. Bar code reader 715 is any known bar code reader capable of reading or scanning a bar code 720, such as a UPC label, associated with merchandise item 710. When the user of WCD 705 scans UPC label 720 with reader 715, WCD 705 acquires a purchase price and an identification code corresponding to merchandise item 710, and stores this information to a memory buffer of WCD 705. As the user scans additional merchandise items while shopping, WCD 705 accumulates a total purchase price in, and adds additional identification codes to, the memory buffer. When the user is done shopping and wishes to pay for the scanned items, the user carries WCD 705 to a POT terminal capable of receiving an electronic transfer of money from WCD 705. The user then initiates a payment process as described in connection with FIG. 4 to pay for the scanned merchandise items at the POT terminal.

In the exemplary e-commerce transactions described above, asset account 110 is a bank account holding money, and money is electronically transferred to/from the bank account. However, asset account 110 can hold other, electronically transferrable, non-monetary assets. For example, asset account 110 can hold electronic coupons, credit points or bonus points cumulatively earned whenever user 105 makes a purchase either in accordance with the present invention, or that is not necessarily in accordance with the present invention. Such coupons, credit points or bonus points can then be applied to subsequent purchases made in accordance with the present invention, wherein the non-monetary assets are electronically transferred to a POT terminal, instead of money. Also, these non-monetary assets can be held in a second or third asset account owned by user 105 in addition to asset account 110. Asset account 110 can also be a credit account, such as a credit card account, for transferring credit to the POT terminal in the e-commerce transaction, thereby obviating the need for a credit card in a credit transaction.

FIG. 8 is a block diagram of an embodiment of WCD 120. WCD 120 has a compact, hand-held form factor similar to that of a personal digital assistant or cellular telephone. The functionality of WCD 120 can be integrated with the functionality of a wireless or cellular telephone so that WCD 120 can be used as both a cellular phone and to effect e-commerce transactions. WCD 120 includes a bus 802 or other communication mechanism for communicating information, and a processor 804 coupled with the bus 802 for processing information. WCD 120 also includes a main memory 806, such as a random access memory (RAM) or other dynamic storage device, coupled to the bus 802 for storing information and instructions to be executed by processor 804. Main memory 806 also may be used for storing temporary variables or other intermediate information during execution of

instructions to be executed by processor 804. WCD 120 further includes a read only memory (ROM) 808 or other static storage device coupled to the bus 802 for storing static information and instructions for the processor 804. A storage device 810, such as a magnetic disk or optical disk, is provided and coupled to the bus 802 for storing information and instructions.

WCD 120 includes display 124, such as a flat panel display, for displaying information to a user. Display 124 is coupled to bus 802. Input device 123, including alphanumeric and other keys, is coupled to bus 802 for communicating information and command selections to the processor 804. Another type of user input device is a cursor control 816, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 804 and for controlling cursor movement on display 124.

Initiation and control of the e-commerce transaction is provided by WCD 120 in response to processor 804 executing sequences of instructions contained in main memory 806. Such instructions may be read into main memory 806 from another computer-readable medium, such as a storage device 810. Execution of the sequences of instructions contained in the main memory 806 causes the processor 804 to perform the process steps described above in connection with FIG. 4 and the exemplary e-commerce transactions described above. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with computer software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

WCD 120 includes a short range, wireless communication interface (I/F) 820 coupled to bus 802. Communication I/F 820 corresponds to the "first interface" mentioned in connection with FIGs. 1 and 7. As described above, communication I/F 820

provides bi-directional wireless data communication with the compatible wireless communication I/F of POT terminal 115, over wireless communication link 137. Communication I/F 820 includes a transceiver for transmitting and receiving data over wireless communication link 137, and a micro-controller for controlling the communication interface. The micro- controller can be integrated with processor 804, and executes program instructions or the like to implement the functionality of the communication I/F including any required data communication protocols. To support alternative arrangement 700 described in connection with FIG. 7, communication I/F 820 can optionally include a known bar code reader.

In the present invention, wireless communication I/F 820 supports digital data packet exchanges between WCD 120 and POT terminal 115, and as such, can be implemented in accordance with exemplary specifications for short-range wireless communications, such as "Bluetooth" and/or Infrared Data Association (IrDA) specifications, or any other suitable specification, so long as a compact communication I/F 820 can comply with the specification requirements. Bluetooth is a proposed radio frequency (RF) specification for short-range, point-to-multipoint data transfer. Bluetooth radio links, operating in the 2.4 gigahertz Industrial-Scientific-Medical (ISM) frequency band, have a nominal communication range between 10 centimeters and 10 meters. However, this nominal range can be extended to 100 meters by increasing the transmit power of a Bluetooth transmitter in communication I/F 820. The IrDA specification provides for wireless data exchanges using a short-range infrared wireless link. Accordingly, a typical distance between WCD 120 and POT terminal 115 during an e-commerce transaction is ten meters or less, unless an extended range transmitter is used in each device.

WCD 120 also includes a wireless network communication I/F 822. Network communication I/F 822 corresponds to the "second interface" mentioned in connection with FIG. 1, and supports the wireless exchange of digital data packets between WCD 120 and network access device 145, as described above. Wireless network communication I/F 822 incorporates a wireless transceiver and a micro-controller similar to the type used in cellular telephony devices for communicating between a cellular telephone and a distant base station. In the preferred embodiment, network communication I/F 822 communicates with network access device 145 using a code division multiple access (CDMA) communication protocol.

It should be understood that POT terminal 115 includes a wireless I/F compatible with wireless I/F 820 of WCD 120. POT terminal 115 also includes a processor and memory sufficient to host and execute server application 345.

While various embodiment of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments and arrangements, but should be defined only in accordance with the following claims and their equivalents.

CLAIMS

1. A method of effecting a wireless electronic commerce (e-commerce) transaction between a wireless communication device and a point-of-transaction (POT) terminal, comprising:

(a) associating unique identifying information with the wireless communications device;

(b) wirelessly transmitting first e-commerce transaction data between the wireless communications device and the POT terminal; and

(c) wirelessly transmitting second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data, from the wireless communications device to a service provider.

2. The method of claim 1, wherein the service provider provides an e-commerce support service to a subscriber having a subscriber asset account electronically accessible to the service provider and remote from both the wireless communications device and the POT terminal, further comprising

effecting a transfer of assets between the subscriber asset account and the POT terminal via the first e-commerce transaction data, the second e-commerce transaction data, and the wireless communications device; and

increasing and decreasing assets in the asset account to reflect the transfer of assets in the e-commerce transaction.

3. The method of claim 2, wherein the subscriber asset account is a subscriber bank account, further comprising

electronically transferring a monetary fund amount from the bank account to the POT terminal; and

determining the monetary fund amount as a function of the first e-commerce transaction data and transaction control commands entered via the wireless communications device to control the transaction.

4. The method of claim 1, wherein step (b) includes

transmitting a request message from the wireless communications device to the POT terminal requesting transaction information from the POT terminal; and

receiving a response message from the POT terminal at the wireless communication device, the response message including the transaction information requested from the POT terminal.

5. The method of claim 4, wherein step (b) further includes transmitting the first e-commerce transaction data over a short-range, wireless communication link in accordance with one of a Bluetooth data transmission protocol, an IrDA data transmission protocol, and a proprietary data transmission protocol.

6. The method of claim 1, further comprising

establishing a wireless network link between the wireless communications device and the service provider in response to receipt of the first e-commerce transaction data at the wireless communications device; and

transmitting the second e-commerce transaction data over the wireless network link using a packet data protocol compatible with an Internet packet data protocol.

7. The method of claim 1, wherein the unique identification information includes at least one of a subscriber personal identification number, a mobile subscriber number, and an electronic serial number, and wherein step (c) includes encrypting

e-commerce transaction data at the wireless communication device using the unique identification information to generate the second e-commerce transaction data.

8. The method of claim 1, further comprising

displaying information relating to the first transaction data at the wireless communications device; and

entering commands via the wireless communications device to initiate and control the e-commerce transaction.

9. A system for effecting a wireless electronic commerce (e-commerce) transaction, comprising:

a wireless communications device having unique identifying information;

a local wireless interface in said wireless communications device for communicating with a wireless interface at a point-of-transaction (POT) terminal;

means for transmitting first e-commerce transaction data between the wireless interfaces; and

means for transmitting second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data from said wireless communications device to a service provider.

10. The system of claim 9, further comprising a support computer at the service provider for providing an e-commerce support service to a subscriber having a subscriber asset account electronically accessible to the support computer and remote from both the wireless communications device and the POT terminal, wherein assets are transferred between the subscriber asset account and the POT terminal via the first e-commerce transaction data, the second e-commerce transaction data, and the wireless

communications device, the support computer including means for increasing and decreasing assets in the asset account to reflect the transfer of assets in the e-commerce transaction.

11. The system of claim 10, further comprising

means for electronically transferring a monetary fund amount from a subscriber bank account to the POT terminal; and

means for determining the monetary fund amount transferred based on the e-commerce first transaction data and transaction control commands entered via the wireless communications device to control the transaction.

12. The system of claim 9, wherein said means for transmitting first e-commerce transaction includes

means in the wireless communication device for transmitting a request message from the wireless communications device to the POT terminal requesting transaction information from the POT terminal; and

means in the wireless communication device for receiving a response message including the requested transaction information from the POT terminal.

13. The system of claim 12, wherein said wireless interfaces include means for transmitting the first e-commerce transaction data over a short-range, wireless communication link in accordance with one of a Bluetooth, an IrDA, and a proprietary data packet transmission protocols.

14. The system of claim 9, wherein the wireless communication device further comprises

means for establishing a wireless network link with the service provider in response to receipt of the first e-commerce transaction data at the wireless communications device; and

means for transmitting the second transaction data over the wireless network link using a packet data protocol compatible with an Internet packet data protocol.

15. The system of claim 9, wherein the wireless communication device further comprises means for encrypting e-commerce transaction data as a function of the personal identification number to generate the second transaction data, wherein the unique identification information includes at least one of a subscriber personal identification number, a mobile subscriber number, and an electronic serial number of the wireless communication device.

16. The system of claim 9, wherein the wireless communication device further comprises

means for displaying information relating to the first transaction data; and

means for entering commands to initiate and control the e-commerce transaction.

17. A system for effecting a wireless electronic commerce (e-commerce) transaction, comprising:

an e-commerce support computer at a service provider for providing an e-commerce support service to at least one subscriber having a subscriber asset account electronically accessible to the e-commerce support computer;

a point-of-transaction (POT) terminal having a wireless interface;

a wireless communications device having

unique identifying information, and including

a wireless interface for communicating with the first wireless interface of the POT terminal,

means for transmitting first e-commerce transaction data between the wireless interfaces of the wireless communication device and the POT terminal; and

means for transmitting second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data between the wireless communications device and the e-commerce support computer.

18. The system of claim 17, wherein the subscriber asset account is remote from both the wireless communications device and the POT terminal, and wherein assets are transferred between the subscriber asset account and the POT terminal via the first e-commerce transaction data, the second e-commerce transaction data, and the wireless communications device, the e-commerce support computer including means for increasing and decreasing assets in the asset account to reflect the transfer of assets in the e-commerce transaction.

19. The system of claim 17, wherein said means for transmitting first e-commerce transaction in the wireless communication device includes

means for transmitting a request message from the wireless communications device to the POT terminal requesting transaction information from the POT terminal; and

means in the wireless communication device for receiving a response message including the requested transaction information from the POT terminal, and wherein

said POT terminal includes means for receiving the request message and means for formulating and transmitting the response message.

20. The system of claim 17, wherein both the wireless communication device and the e-commerce support computer further comprise means for encrypting e-commerce transaction data as a function of unique identification information to generate the second transaction data, wherein the unique identification information includes at least one of a subscriber personal identification number, a mobile subscriber number, and an electronic serial number of the wireless communication device.

21. A computer program product comprising computer usable media having computer readable program code means embodied in said media for causing application programs to execute on computer processors in a wireless communication device, in a point-of-transaction terminal, and in an electronic commerce (e-commerce) support computer at a service provider, to effect an e-commerce transaction, said computer readable program code means comprising:

a first computer readable program code means for causing the processor to associate unique identifying information with the wireless communications device;

a second computer readable program code means for causing the processor to wirelessly transmit first e-commerce transaction data between the wireless communications device and the POT terminal; and

a third computer readable program code means for causing the processor to wirelessly transmit second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data, from the

wireless communications device to the e-commerce support computer.

22. The computer program product of claim 21, wherein the second program code means includes computer readable program code means for causing the processor to encrypt e-commerce transaction data as a function of the personal identification number to generate the second transaction data, wherein the unique identification information includes at least one of a subscriber personal identification number, a mobile subscriber number, and an electronic serial number of the wireless communication device.

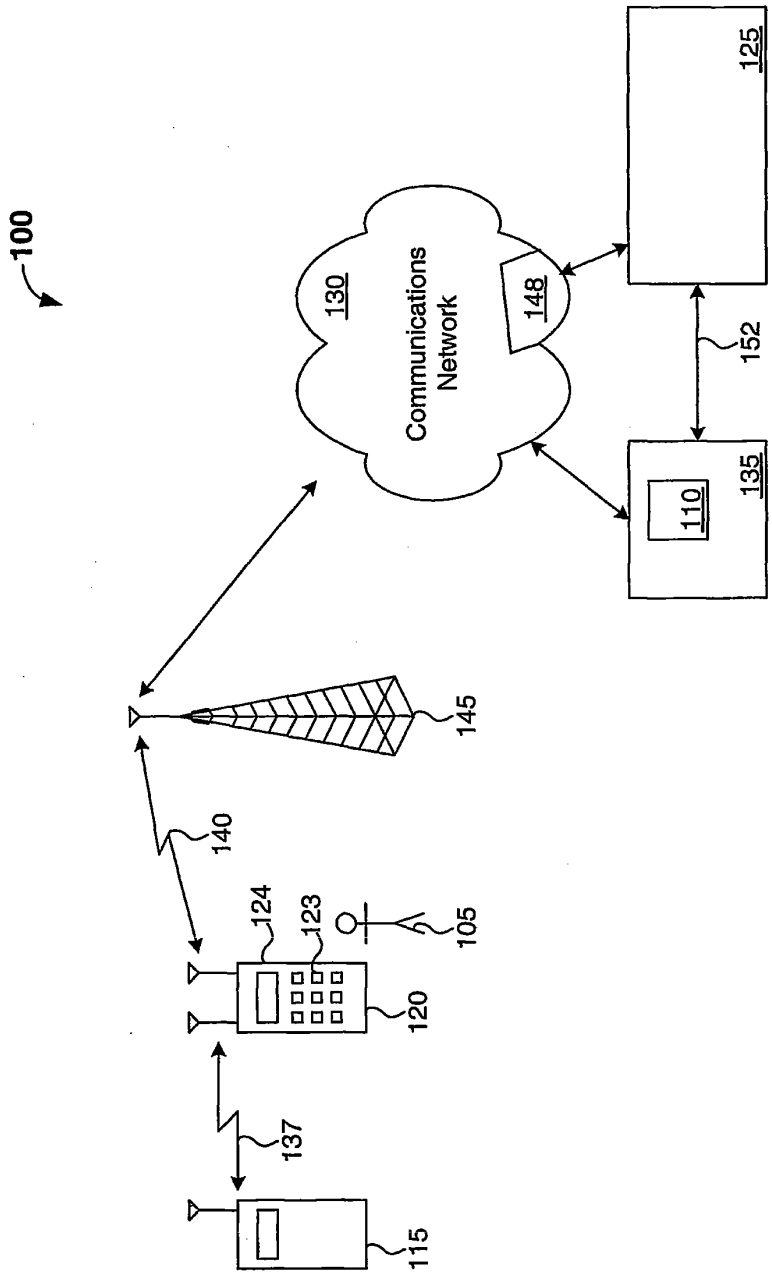

100
130
Communications Network
148
125
152
135
110
145
140
124
123
105
120
137
115

FIG. 1

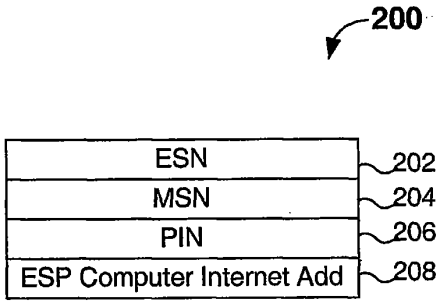


FIG. 2A

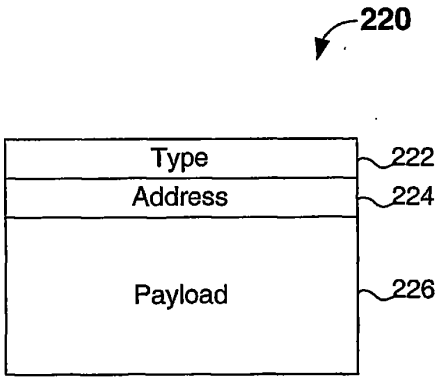


FIG. 2B

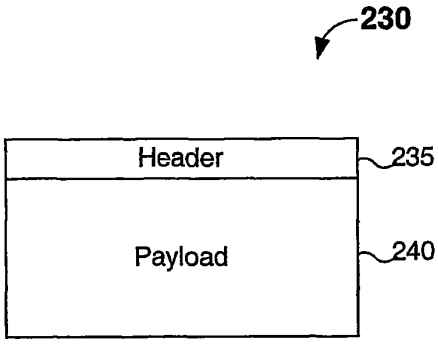


FIG. 2C

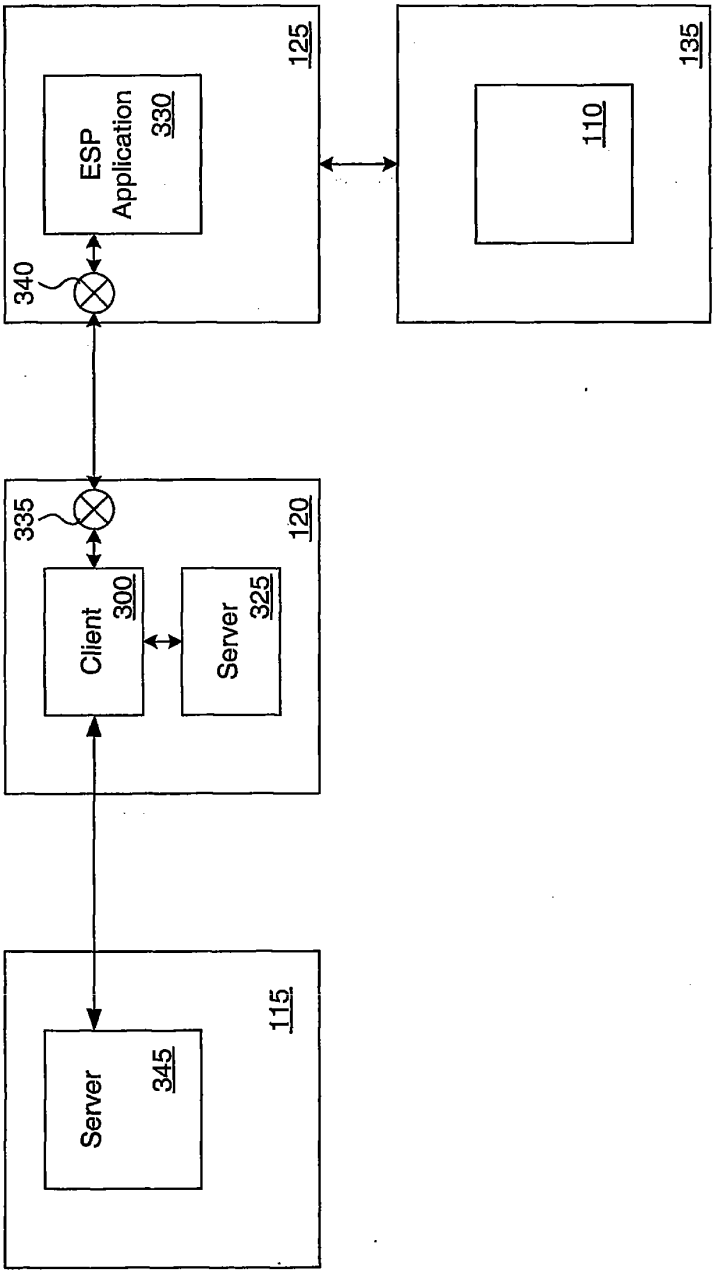

125
ESP Application 330
340
135
110
335
120
Client 300
Server 325
115
Server 345

FIG. 3

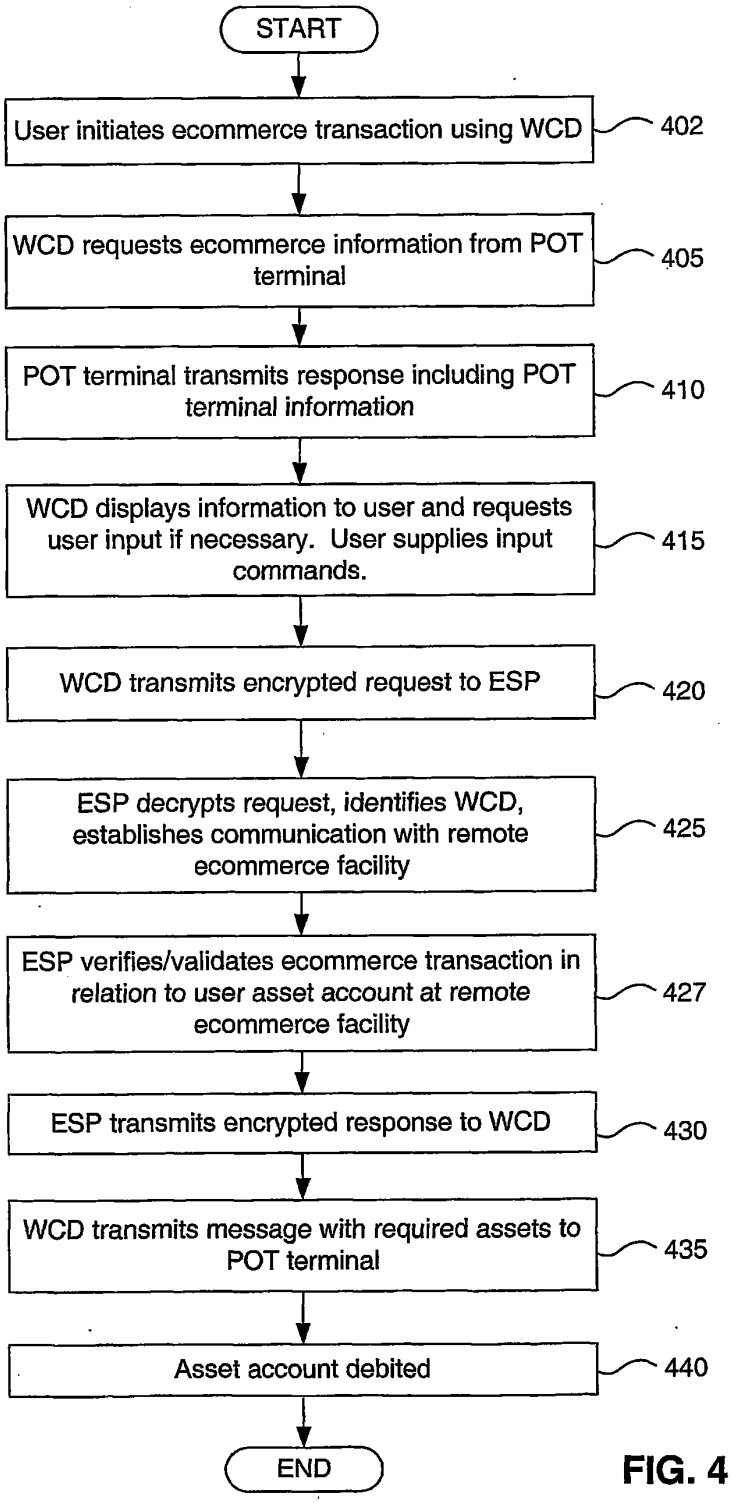

START
User initiates ecommerce transaction using WCD
402
WCD requests ecommerce information from POT terminal
405
POT terminal transmits response including POT terminal information
410
WCD displays information to user and requests user input if necessary. User supplies input commands.
415
WCD transmits encrypted request to ESP
420
ESP decrypts request, identifies WCD, establishes communication with remote ecommerce facility
425
ESP verifies/validates ecommerce transaction in relation to user asset account at remote ecommerce facility
427
ESP transmits encrypted response to WCD
430
WCD transmits message with required assets to POT terminal
435
Asset account debited
440
END

FIG. 4

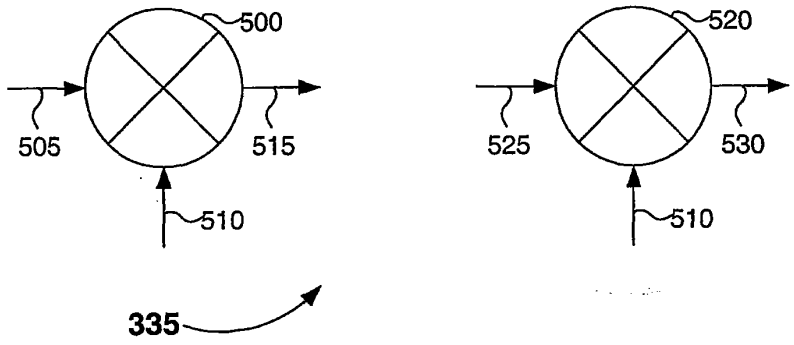


FIG. 5

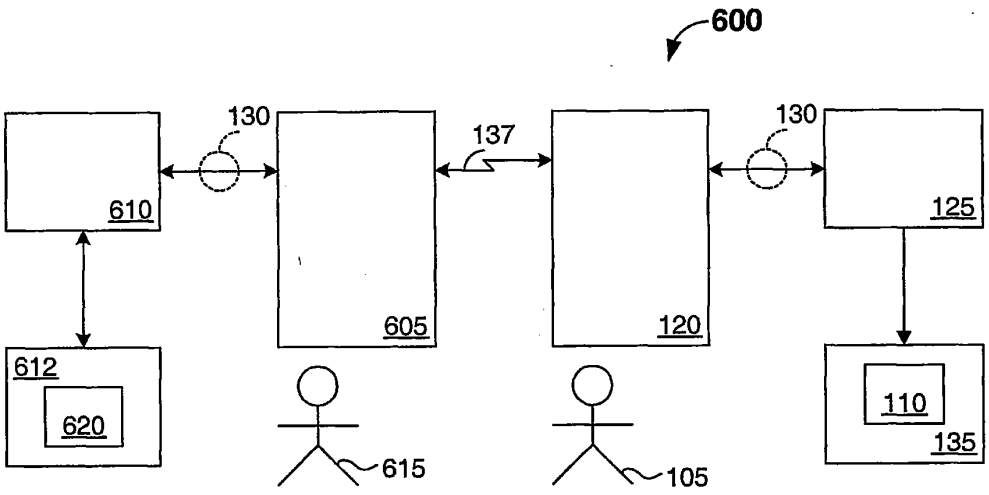


FIG. 6

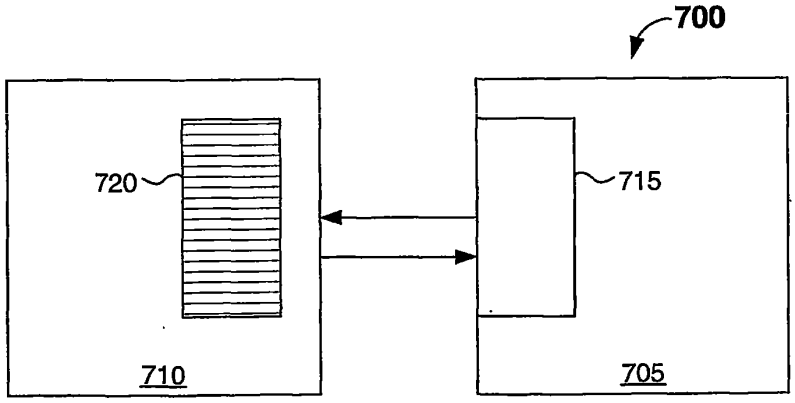


FIG. 7

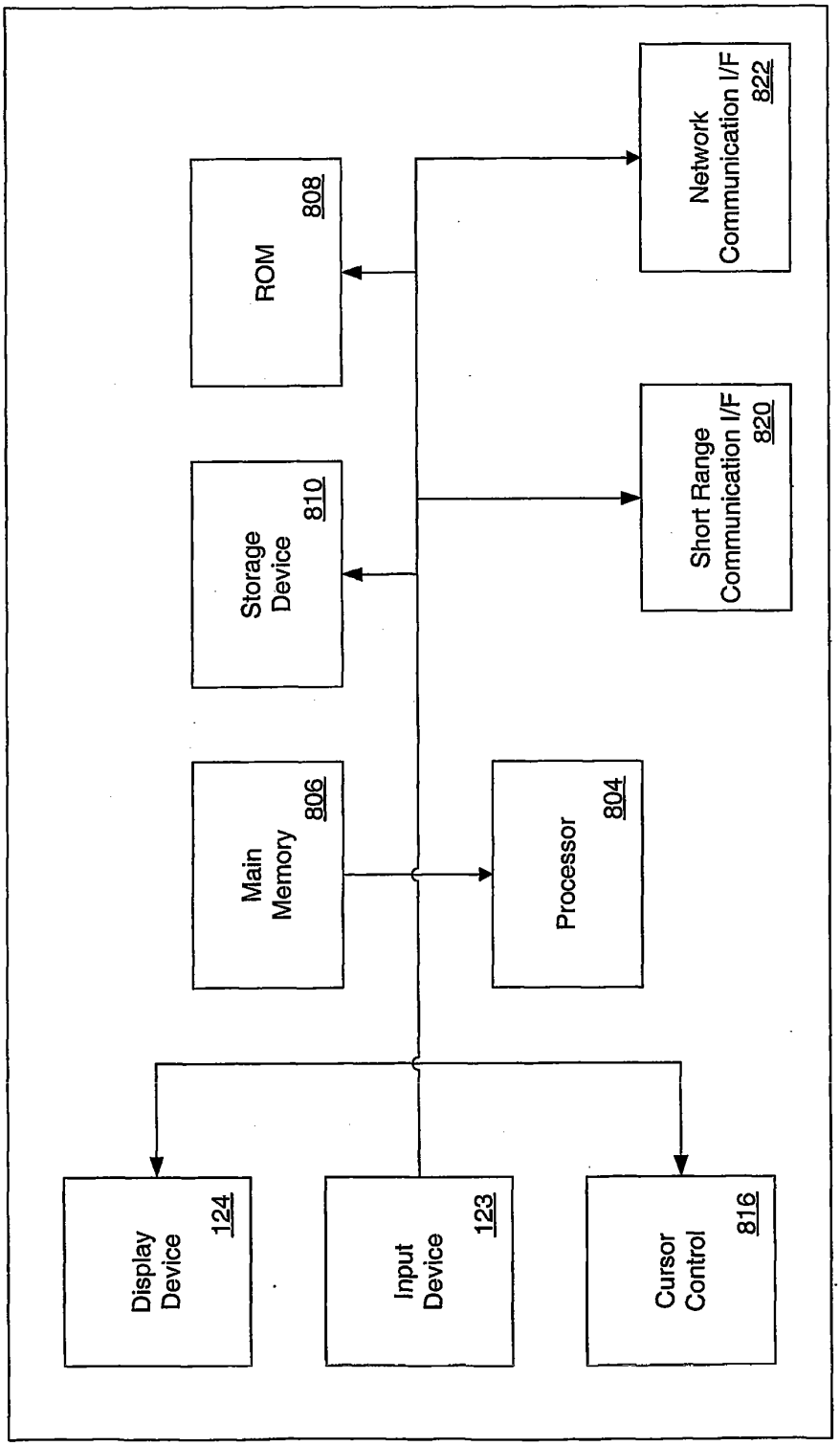

Network Communication I/F 822
ROM 808
Short Range Communication I/F 820
Storage Device 810
Main Memory 806
Processor 804
Display Device 124
Input Device 123
Cursor Control 816

FIG. 8

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04M 17/00, H04Q 7/32

A1

(11) International Publication Number: **WO 99/13636**

(43) International Publication Date: 18 March 1999 (18.03.99)

(21) International Application Number: PCT/GB98/02729

(22) International Filing Date: 10 September 1998 (10.09.98)

(30) Priority Data:
9719100.1 10 September 1997 (10.09.97) GB

(71) Applicant *(for all designated States except US)*: TEKTON COMMUNICATIONS LIMITED [GB/GB]; Marsh House, 500 Montagu Road, London N9 0UR (GB).

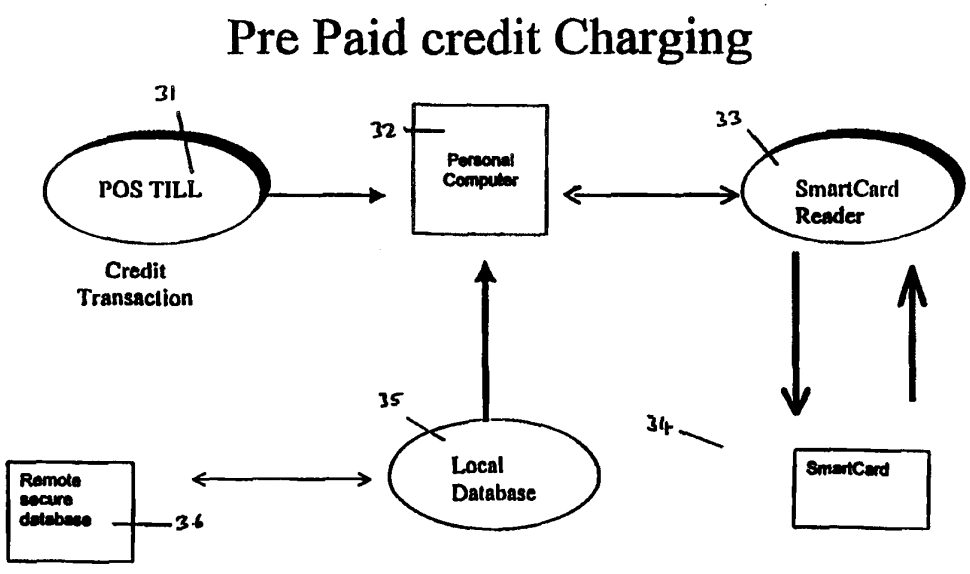
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BISWELL, Anthony, James [GB/FR]; Villa Mas Souleou, Boulevard Plan des Abeilles, F–06230 Saint Jean Cap Ferrat (FR). CASTLE, Derek, Keith [GB/GB]; 4 Tavern Road, Wooley Bridge, Glossop, Derbyshire SK13 2RB (GB).

(74) Agent: COATES, Ian, Harold; Sommerville & Rushton, 45 Grosvenor Road, St. Albans, Herts AL1 3AW (GB).

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

Published
With international search report.

(54) Title: A PRE–PAYABLE COMMUNICATION DEVICE



(57) Abstract

A portable radio communications apparatus comprising: (i) a portable handset; (ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit; (iii) a recess in the handset adapted to accept the removable module; (iv) a reading device in the handset adapted to determine a content of the electronic purse; (v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse; and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A Pre-payable Communication Device

Field of Invention

The present invention relates to pre-payable communication devices and more particularly to pre-payable communication devices which are suitable for use in radio communication networks.

Background to the invention

One problem with radio communication devices such as mobile telephones is that they are relatively expensive both to purchase and to run. This represents a problem both for the subscriber and for the service provider. For example, the service provider needs to rely on the creditworthiness of the mobile phone subscriber and both the service provider and the subscriber are at risk from fraudulent use of the subscriber's terminal. Many people who would otherwise benefit from the occasional use of a mobile phone are prevented from having this benefit because either the cost is too high and/or the service provider is unable to rely on their creditworthiness. For occasional users the monthly line rental charge is often prohibitively expensive.

There are many situations in which the use of conventional mobile telephones is problematic. For example, an employee may be given a mobile telephone by his employer to use only in essential circumstances. The employer would like to ensure that the employee does not run up additional costs by using the phone for personal use. However, this is difficult to do until after the event when the employer is able to check the telephone bill.

Another problem relates to the fact that in different geographic locations, different communication protocol systems are in operation. An example of a protocol system is Global system for Mobile Communications (GSM) which is a European protocol system. Typically, mobile telephone handsets are operable with only one, or perhaps two different communication protocol systems. This means that when the user

APPL-1002
APPLE INC. / Page 564 of 1892

moves to a different geographical area, he may be unable to operate his mobile telephone, if the communication protocol system for that area is incompatible with his handset. This is often a problem for travellers and yet travellers often only have access to mobile communications devices and need them most when they are on the move.

Some attempts have been made to overcome these problems using SmartCard technology. A conventional SmartCard is typically a rectangular piece of plastics material, of a similar size and shape to a credit card, which contains integrated circuits, microprocessors and/or read write memory. The use of SmartCards in radio telephones is known, for example, as described in UK patent application number 2267794 in the name of Alan Kilpatrick Conroy. This application describes a pre-payable mobile cellular phone. However, the specification gives no details on how the pre-payment is achieved.

UK Patent 2266798 in the name of Motorola Inc. describes an apparatus for accepting, retaining and making electrical contact between a SmartCard and a radio telephone handset. The SmartCards used in radio telephones have been limited to subscriber identification module (SIM) cards for use in the European market. SIM cards are available in two sizes; a full size card and a chip card. SIM cards for GSM currently provide subscriber information (e.g. subscriber phone number, service provider) and plug into a GSM compatible mobile telephone handset to configure that handset for a particular subscriber. These cards only reference the subscriber data and do not include radio frequency circuitry or protocol information. If the SIM card is removed from the handset incoming calls cannot be received.

International patent application number WO/97/05729 in the name of Telecom Italia Mobile S. P. A. describes a radio mobile terminal that is provided with two SIM card readers. One of the SIM cards is described as a prepaid card and this can be loaded into the additional reader. This system is disadvantageous because the mobile

APPL-1002
APPLE INC. / Page 565 of 1892

telephone handset needs to contain two SIM card readers which increases the cost and bulk of the terminal. Also the design of the handset is complex because two SIM card readers must be allowed for.

None of the above prior art provides either communications equipment or a method of operation which enables every would-be subscriber, regardless of creditworthiness to have access to a mobile phone on a pay-as-you-use basis.

It is accordingly an object of the present invention to provide a pre-payable communication device for use with radio communication networks and a method of using such equipment which overcomes or at least mitigates one or more of the problems noted above.

Summary of invention

According to the present invention, there is provided a portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed. This gives the advantage that every would-be subscriber, regardless of creditworthiness can have access to a mobile phone on a pay-as-you-use basis. When the module is removed from the device, the communications apparatus is inoperable which helps to prevent fraud. The subscriber

identification unit in the removable module provides "identification" for a particular subscriber, so that one subscriber can use several different handsets and configure these for his own use simply by adding the removable module. This helps subscribers when they travel between areas covered by different protocol systems. Such a traveller would be able to retain his or her removable module and simply insert this into a different handset that is operable with the new protocol system.

Preferably, the removable module comprises a SmartCard. This provides the advantage that the removable module is conveniently sized and shaped and can easily be stored and transported.

In one embodiment of the invention the subscriber identification unit comprises a conventional subscriber identification module. This provides the advantage that the subscriber identification unit can easily be obtained and is compatible with other known systems. Preferably the subscriber identification unit is adapted to be compatible with the Global System for Mobile Communications Protocol. This enables the communications apparatus to be used with a widely used European protocol system.

According to another aspect of the present invention there is provided a removable module suitable for use with a portable radio communications handset said module comprising an electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus. This provides the advantage that removable modules are provided which contain an electronic purse. Would-be subscribers can obtain a removable module, regardless of their creditworthiness, and use this to gain access to a mobile phone on a pay-as-you-use basis.

According to another aspect of the present invention there is provided a method of communicating using a portable radio communications apparatus said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation. This provides the advantage that a service provider or air-time provider no longer needs to be responsible for the creditworthiness of all its subscribers. Individual subscribers may purchase air-time units using cash and "charge" a removable module in this way. The "charged" module can then be used to communicate using the mobile phone handset. The subscriber is then able to use the handset on a pay-as-you-use basis.

The present invention is intended to encompass both the removable module and the handset together and individually. The invention also encompasses a method for using the removable module and handset as well as a charging station for charging the removable module.

Description of the drawings

The invention will be further described, by way of example, with reference to the accompanying drawings in which:

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus.

APPL-1002
APPLE INC. / Page 568 of 1892

Figure 2 is a schematic diagram of a handset and removable module.

Figure 3 is a flow diagram showing a method of recharging a removable module.

Figure 4 is a flow diagram of actions and screen messages in a method of recharging a removable module.

Figure 5 is a flow diagram of actions and screen messages in a method of initialising a removable module.

Figure 6 is a schematic diagram of an external fraud detection system.

Figure 7 is a schematic diagram of an alternative external fraud detection system.

Description of preferred embodiments

Embodiments of the present invention are described below by way of example only. These examples represent the best ways of putting the invention into practice that are currently known to the Applicant although they are not the only ways in which this could be achieved.

Figure 2 is a schematic diagram of a portable radio communications apparatus 20 comprising a portable handset 21 and a removable module 22. The portable handset is shown as being similar to a conventional mobile telephone handset although any suitable type of handset may be used. In the example shown the handset comprises a display area 23, an aerial 24, a key pad 25 and a recess 26. The recess 26 is adapted to receive the removable module 22 as shown in figure 2. The handset may also comprise a microphone and a loudspeaker (not shown) as well as other elements typically contained in a conventional radio telephone handset. However, in one embodiment of the present invention, some components that would typically be contained in a conventional radio telephone handset are removed from the handset 21 and replaced by equivalent or alternative devices and circuitry in the removable module. This is explained further below.

APPL-1002
APPLE INC. / Page 569 of 1892

The removable module 22 is shown as being generally rectangular in shape although any shape can be used. Preferably the removable module is a SmartCard and has a shape similar to that of a conventional credit card. The removable module comprises an electronic purse. The term "electronic purse" is used to refer to any form of memory that is capable of being read and updated, and which is capable of storing information about units of "air-time". Preferably, the electronic purse is rechargeable, that is once the units of "air time" that it contains have been used up, they can be replaced. However, this is not essential. The removable modules can be disposable, so that once the units are used up the module is simply replaced. Units of "air-time" are units of time for which a communications service is provided by a communications network service provider. The removable module 22 can be inserted into and removed from the recess 26 in the handset.

The removable module 22 also comprises a subscriber identification unit (not shown) which is preferably a conventional subscriber identification module (SIM). For example, the removable module 22 can be a SIM card which further comprises an electronic purse. When the removable module 22 is removed from the handset the SIM is also removed and this means that the communications apparatus 20 cannot be used to transmit or receive information. When the SIM is removed from the apparatus 20 there is no information in the handset about which subscriber is using the apparatus, for example, the user's telephone number. This means that the communications apparatus is substantially inoperable when the module is removed.

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus. This represents one example of a method for using the prepayable portable radio communications apparatus; other methods may also be used. The user first obtains a removable module 22 and inserts this into the handset 22 and then a card validity check process 1 is carried out. The card validity check process

involves checking whether the removable module is in anyway "data corrupt" or is not in credit. The handset contains a reading device adapted to determine a content of the electronic purse and also an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse. At this stage it is also possible for the subscriber to key in a personal identification number (PIN) to the key pad of the handset in order to allow use of the removable module. This provides extra security for the subscriber because it prevents unauthorised use of the removable module and/or the handset. However, use of a PIN number in this way is optional.

The next stage 2 involves a network authentication check by the airtime provider. This involves a check of the information provided in the subscriber identification unit or SIM (if a SIM is used). By making this check the service provider can help to prevent use of fraudulent removable modules. If the result of stage 2 is a "fail" i.e. the check is unsuccessful for any reason then the communications apparatus is not enabled as shown in box 3 in figure 1. That is, the enabling means prevents use of the communications apparatus. A warning message and instructions to the subscriber can be displayed on the display panel to indicate that access to the communications network by the service provider has not been granted.

If the result of stage 2 is successful then full functionality and dial facilities are granted by the service provider as indicated in box 4 of figure 1. The subscriber is then able to use the portable radio communications apparatus and as information is transmitted or received from the apparatus (indicated by box 7 in figure 1) the electronic purse is updated (as indicated by arrow 10 in figure 1). For example, as units of "air time" are used by the subscriber these are decremented from the electronic purse contents. Once the reading device determines that the electronic purse is empty the result of the airtime credit box 5 is a "fail" and the user is advised (box 6) and the

enabling device prevents use of the communications apparatus. At this point the user may remove the removable module from the handset and use a charging station to recharge the module. That is, the user may purchase more "air-time" units and store these in the electronic purse on the removable module.

This method provides the advantage that the service provider is not responsible for the creditworthiness of the subscriber. Also, the subscriber is able to use a mobile phone on a pay-as-you-use basis and is fully in control of his or her expenditure at any one time. It is not necessary for the whole mobile telephone to be configured for use specifically by one subscriber i.e. the telephone does not have to be configured for one telephone number. This is because the telephone number effectively "travels with" the subscriber within his removable module. When the subscriber moves between geographical regions over which different communications protocols are used the subscriber can simply obtain a new handset, that is preconfigured for the protocol of that area, and insert his removable module into the handset in order to configure that handset for his own personal use. For example, travellers could hire a telephone handset when they enter a new area.

The charging station comprises a recess which is able to accept a removable module and also means for entering "air-time" units onto the electronic purse on the module.

As described above, in one embodiment of the invention, some of the functionality from the handset is removed and placed onto the removable module. That is, the handset will typically contain electronic apparatus which will enable the handset to function as a radio communications apparatus when the electronic purse is "charged" and the subscriber identification unit is provided. This means that the handset is hugely more expensive relative to the removable module. However, in one embodiment of the invention, some of the functionality from the handset is removed and instead

incorporated into the removable module or SmartCard. This increases the value of the removable module relative to the handset and may also ensure that the handset will not function without the removable module. Examples of functions that could be removed from the handset include the enabling means, the reading device and other features such as circuitry for converting the speech signal from the user into digital form. These are only examples of functions that could be incorporated into the removable module. Other functions could also be incorporated by making use of conventional circuit design techniques such as would be know to the skilled person in the art.

By making the removable module more expensive with respect to the handset itself, the risk of theft of the handset is reduced and the consequences of theft of the handset are less severe.

In one example, the present invention is made available as an integral component of a customer loyalty programme. The pre-pay mobile telephone is made available to loyalty card holders as an extension of any existing loyalty scheme, on the basis of reward for tenure and spend within the loyalty scheme. Users are able to earn loyalty points on airtime and also to redeem loyalty points against purchase of airtime.

In this example of the invention, the SmartCard for use with the pre-pay mobile telephone handset is also functional as a customer loyalty card. The SmartCard contains an amount of airtime included at the time of purchase and subsequent recharging of the card is possible upon each visit to the loyalty scheme provider's premises.

A number of advantages are provided to the loyalty scheme provider including:

- provision of an "added value" service to existing customers
- ability to attract new customers
- broad customer availability - no credit rating checks
- rechargeable only at loyalty scheme provider's retail outlet

APPL-1002
APPLE INC. / Page 573 of 1892

- minimal overheads and capital expenditure
- use of airtime derives gross revenues prior to month end settlement
- information about customers behaviour patterns is gained

Recharging the removable module

Figures 3 and 4 are flow diagrams which illustrate the process of recharging the removable module or SmartCard. When the user needs to recharge his or her SmartCard 34 he or she visits the loyalty provider's premises and at a point of sale till 31 carries out a credit transaction 41, 42 to pay for airtime units to be charged onto the SmartCard 34. After removal from the handset 43 the SmartCard 34 is then inserted 44, 45 into a SmartCard reader 33 that is connected to or integral with a secure personal computer 32. The personal computer 32 is connected to a local database 35 which contains information about the user's loyalty card and SmartCard 34. The local database 35 is in turn connected to a remote secure database 36.

A message 46 is displayed on the screen of the personal computer 32 which indicates the amount of pre-paid air time units that remain on the SmartCard 34. The amount of air time units that are to be credited to the card 34 is then entered onto the personal computer 46 and the personal computer updates the electronic purse in the SmartCard 34 accordingly using an encrypted transaction. The amount of units to be credited to the card can either be entered manually or can be transferred electronically from the till 31 to the computer. The updated amount of pre-paid air time units on the SmartCard 34 is displayed on the computer screen 47 and the SmartCard 34 is then returned to the user or customer 47. Finally the handset is returned to the customer 48. The encrypted transaction involves the following steps:

1. The secure personal computer obtains secret data that is specific to the SmartCard from the SmartCard itself and/or the local and remote databases and builds an encrypted update command.

2. The software within the card deciphers the encrypted command and updates the airtime counter or electronic purse within the SmartCard.

Such an encrypted transaction is recorded by the personal computer and when a batch of such records are obtained this batch is sent to the remote secure database 36 for storage and to update that database.

Initialising the removable module

Each SmartCard contains secure key information which is stored on the card during the manufacturing process. Information about these secure keys is held on the main database 36 and is accessible by the local database 35.

When a user first obtains a removable module or SmartCard 34 this is initialised by placing the SmartCard 34 into the card reader 33. Information from the card 34 which identifies the card and provides security information (i.e. the secure key) is read by the card reader 33 and checked by the personal computer 32 using information from the local and/or remote databases 35, 36.

If this check is successful the card if authenticated 55 and a screen message asking for loyalty card details to be entered is displayed 55. The loyalty card details are entered 52 to the personal computer 32 and then the card is initialised by the personal computer 53. Details linking the loyalty card details and the secure key are stored on the local and/or remote database 35, 36 and an initial amount of airtime credit is charged to the card. The card is then removed from the reader and returned to the customer 57 in order to be inserted into the customer handset 54.

External fraud detection system

A fraud detection system is provided that is external to the handset and removable module. This is provided in addition to any fraud detection system provided by the network operator. This system monitors traffic made on the pre-paid mobile telephone network and compares this traffic against information about recharging of

SmartCards on the system. For a particular SmartCard, if more traffic is being created than is justified by the amount of credit on that SmartCard then possible fraud is identified. After checks have been made, if it is found that fraud is occurring then the SmartCard is prevented from accessing the network.

Figures 6 and 7 show two examples of an external fraud detection system. Pre-paid mobile phone handsets 62 are used to communicate over an operator or service provider's communications network 61. Each time a call is made a call detail record (CDR) is created and stored by the operator 61, as is known in the art. A call detail record contains information about the calling party, the called party, the duration of the call, the time when the call was made and other information about the call. At the end of a certain period of time, for example 12 hours, the call detail records for that 12 hour period are downloaded to database 66,71 in the fraud management system.

A SmartCard reader 64 or other removable module reader is provided that is connected to a till 63 such that the card reader 64 and till 63 are uniquely matched for security reasons. When a SmartCard or removable module is recharged using the card reader 64 and till or PC 63 information about the recharge is downloaded to a database 65, 71 in the fraud management system. Information about new users from the card initialisation process can also be downloaded. The information can be stored within the local database 35 before being downloaded in batches.

In the example shown in figure 6 the fraud detection system comprises two separate databases 65 and 66. One database 66 stores the call detail records and the other 65 stores information about credit data and new users. The information from these two databases is accessed and compared by a processor 67 in order to identify potential fraud cases. The processor 67 generates action requests and reports of fraudulent activity. These outputs can be provided directly to a human operator 69 or

APPL-1002
APPLE INC. / Page 576 of 1892

can be sent to the network operator 61. Information from the databases 65, 66 and processor 67 can also be provided to the clubcard database 68.

In the example shown in figure 7 a single database 71 is used which stores information about both call detail records and credit data. The network operator 61 has access to information from this database 71 as shown in figure 7. The database 71 also comprises a processor for analysing the data and producing management reports 73. Real time access 72 to the database 71 can also be provided.

Because there is a time delay whilst data enters the database(s) 71, 65, 66 then the database may state that no credit remains on a particular SmartCard, when in fact the user has recently recharged the SmartCard. Allowance is made for this in order to avoid detecting this situation as a case of fraud. This is described below.

The processor 71, 67 in the fraud management system is arranged to detect a potential case of fraud in situations such as:

- the total number of calls made for a particular SmartCard in a predetermined period exceed a threshold level;
- the total number of units used in a single call exceed a threshold level;
- the number of calls to a free helpline number exceed a threshold level;
- calls have been made by a user who has been barred or for whom a tamper alert has been generated by "in store" card reader systems;
- if a barred type of call set up is detected such as a call transfer;
- if the number of a certain type of outbound call events generated by a user or group of users exceeds a threshold;
- if the number of inbound verses outbound call events, in a given period, by a user or group of users falls within a certain range.
- if multiple use of a handset or SmartCard is detected from CDR data; and

- if geographically improbable use of a handset or SmartCard is detected from CDR data.

The interfaces to and from the fraud management system are now described.

Interfaces

- Imports of Call Detail Records (CDR) data from the network operator are performed on either a chronological push or pull basis at intervals that are viable by the system owner.
- Imports of "credit accumulated" data are performed on either a chronological push or pull basis at intervals that are variable by the system owner.
- Import of tamper alerts or "excess credit accumulated" general action requests for termination to the network operator.
- Export of management information reports and action requests to external systems located at the operator or at the system owners premises are performed on either a chronological push or pull basis at intervals that are variable by the system owner.

The fraud detection system itself is protected from unauthorised access by Firewall Security on call External Data Communications.

Security

- The fraud detection system is protected from unauthorised access by firewall security on all external data communications.
- Physical access to the system is only possible by authorised personnel who are required to pass security vetting procedures.
- Back up of the system data is performed at regular intervals and back up data is stored at a secure off site location.

APPL-1002
APPLE INC. / Page 578 of 1892

Use of handset and removable module to monitor the duration of calls

Because the CDRs are downloaded to the fraud detection system at intervals, such as 12 hourly or 2 hourly intervals, then a time window is present during which fraudulent use of "unpaid for" airtime may occur. In order to reduce this problem the handset and removable module combination is able to monitor call durations during this time window. If more than a threshold level of total call duration is exceeded during this time window than a potential fraud is detected. In this event the communications apparatus is either shut down until the time window has passed or the network operator or security staff are alerted.

This is implemented by incorporating a timer mechanism into the removable module or SmartCard. At the start of a call a pulse signal is sent from the handset to the module and this activates the timer mechanism. At the end of a call another pulse signal is sent from the handset to the module to deactivate the timer. The timer thus monitors total call duration for all calls during a time window, after which it is reset to zero. A processor in the removable module or SmartCard compares the call duration value from the timer against a predetermined threshold and if the threshold is exceeded all outgoing calls are barred for the duration of the time window.

The time window, or exclusion time is set from within the handset/SmartCard combination. At the end of this time normal outgoing call usage is restored and the process counters are reset to zero time.

If the total call duration time as monitored by the handset and module is less than the prescribed threshold then no action is taken to terminate outgoing calls.

Emulation of advice of charging signals

In the situation that no pulses or signals are provided by the network operator which contain information about the current charging rates then the handset and

APPL-1002
APPLE INC. / Page 579 of 1892

SmartCard combination is able to emulate these signals. For example, this is required when charging signals are blocked, disrupted or not provided.

A timer mechanism is provided in the handset or in the removable module in order to emulate the charging signals. This timer may be the same as the timer described in the section headed "use of handset and removable module to monitor duration of calls" above. This timer mechanism is activated by signals from the handset which are provided at the start and end of a call. Information about tariff rates is stored in the handset or removable module. For example, this information can be stored in the form of a look up table. Time information from the timer mechanism is then used in conjunction with the tariff information in order to determine the cost of the call. The electronic purse is then decremented accordingly.

Other security features

- The handset is provided with two personal identification number accesses. A first PIN access allows the handset to be activated and a second provides access to sub routings which can change values such as the value of charges or amount of charge time.
- Certain types of call, such as those to 0891 numbers may simply be barred to help prevent fraud.
- A particular handset and removable module or SmartCard are electronically "locked" together during the manufacturing process so that they may only be used in conjunction with each other. This is done by storing a secure key in either or both of the handset and the removable module or SmartCard. The secure key is a cryptogram or other encrypted code. Means for checking that this secure key is present and correct are provided in the handset or removable module. Each handset and module pair is given a unique key so that they will only function fully together. The term "key" is used to refer to stored cryptograms, encoded

APPL-1002
APPLE INC. / Page 580 of 1892

information and other electronic keys as well as physical apparatus which ensures that a particular handset can only be used with a module which is able to operate the key.

SmartCard

Details about the SmartCard are described below:

Functionality

The SmartCard provides the means for storing an amount of credit in agreed currencies or units of time up to predetermined maximum values, which are variable by secure communication to a SmartCard reader. The credit is debited by the operation of a mobile telephone or by a card reader in a point of sale terminal.

The SmartCard provides control over the mobile Handset functions of:

- Network authentication per the GSM protocols.
- Phone book directory per Handset implementation.
- Short message service.
- Handset welcome and permanent message display
- Confirm that the credit remaining prior to call set up is above a pre-set threshold value held on the SmartCard, and prevent call set up if below this value.
- Monitor credit remaining for a call in progress, decrement the credit at specific usage rates derived from an advice of charge, (AOC) trigger signal on the signalling channel and interrogate the tariff information stored on the SmartCard. The network operator sends out signals which provide information about the charging rate. Examples of these signals are AOC or CAI (charging advice information). Any such type of signal can be used to enable the credit to be decremented correctly.
- Monitor total duration of calls made in a period and prevent additional calls until this period is expired, excluding all zero rated calls.

APPL-1002
APPLE INC. / Page 581 of 1892

- Monitor call in progress duration, provide user warning and tear down when threshold reached.
- Holding pre-determined call limits and monitoring all calls made over a given period, and of a given duration, to allow for call barring should these pre-determined thresholds be exceeded. This is described in detail in the section headed "use of handset and module to monitor the duration of calls"
- The SmartCard is able to place restrictions that allow single language selection only.
- Provide advice of charge (AOC) charging information to the handset, when AOC emulation is used in the handset firmware for those instances where AOC is not presented or supported by the network.
- The SmartCard is able to hold a secure electronic purse function that is capable of managing and controlling units of currency that are stored within it.
- The SmartCard is capable of storing loyalty or other retailer defined units as "points" which may have no monetary value placed upon them. These "points" are redeemable via the SmartCard reader as units to be used in Prepay systems.

Interfaces

- A set of interface protocols are defined for secure transactions between the Handset and the SmartCard, to prevent fraud either through spoofing, or tamper of either the Handset or the SmartCard.
- A set of interface protocols are also defined for secure transactions between the card reader and the SmartCard, to prevent fraud either through spoofing, or tamper of either the card or the card reader.

Security

- No information generated by the SmartCard to the Handset relating to prepay usage is transmitted to the network by the radio interface or by any other means.

APPL-1002
APPLE INC. / Page 582 of 1892

- The SmartCard is capable of detecting unauthorised tampering and ceases to function until returned to a card reader and reactivated. For example, if the wrong personal identification number is entered three times during the card validity check process.
- The SmartCard protocols prevent no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- A limited number of master SmartCards may be provided for use by point of sale operators, issued under strict controls in store.
- A number of secure access modules (SAM's) for use in the card readers at point of sale can be provided. A SAM is a fixed SIM which contains cryptograms for accessing the identity or secure key information from the SmartCards.

The SmartCard:

- Allows remote disablement of the Handset and SmartCard upon authenticated request by the network or by the card reader.
- Allows remote enabling of the Handset and SmartCard upon authenticated request by the network or by the card reader in combination with user PIN entry.
- Does not allow re-enablement of the SmartCard once it has been disabled.
- Allows remote individual update of the threshold values held in the SmartCard, either by the card reader or over the network.
- Does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2 of the handset.
- Does not suffer any electrical or physical damage if withdrawn from the Handset or Card reader, while power is applied. The SmartCard retaining unit, in one embodiment, has retaining pins that are close together. The retaining unit is specially designed such that these pins do not flex and contact each other, so creating a short circuit.

APPL-1002
APPLE INC. / Page 583 of 1892

- Is delivered pre-registered with the network operator but not activated for use. Activation is only possible via the Card Reader.
- Permits Incoming calls when the credit has expired.

Standard Functions NOT required on the Card

Standard functions that are not required on the SmartCard, such as phone book options can be removed in order to make room for extra filters or algorithms for coding or decoding encrypted information.

- Phone Book Options

Form factor

- The SmartCard can be a full size SIM, mini SIM adapter based alternatives are also possible.
- The SmartCard can be delivered with a surface finish or other orientation mark to assist in identification of its correct insertion for visually impaired users.

Appearance

- The SmartCard can be capable of accepting various finishes e.g. silk screen printing for branding.
- In one embodiment each SmartCard is individually marked with a machine readable bar code and human readable serial number. Records of all SmartCard serial numbers and their distribution can then be kept.

SmartCard Reader

Functionality

The SmartCard reader:

- Allows SmartCards to be activated for first use and recharged with credit on a periodic basis. Allows SmartCards to be deactivated by the operator or automatically upon detection of tampering within the SmartCard by the SmartCard reader system.

APPL-1002
APPLE INC. / Page 584 of 1892

- Allows the operator to read from a SmartCard remaining credit on a card inserted in the reader.
- Captures and temporarily stores the credit held on the card and the subscriber phone number to allow transfer to a replacement card.
- Allows transfer of credit remaining on the SmartCard to a new card or to a secure external system for point of sale transactions.
- Is intuitive to use by semiskilled checkout operators with a minimum of training, and employs the use of icons to indicate functions where possible.
- Is easily serviced by trained personnel, with a good supply of replacement parts and spares.
- The SmartCard reader allows a secure sign-on process at power on, user log on and log off. This process involves the use of master SmartCards coupled to PIN number entry.
- The SmartCard reader is capable of maintaining the system clock function to allow for daylight saving.
- The SmartCard reader is capable of recording the operator name and sign on/off date/times.
- The SmartCard reader has a supervisor login password for password administration.
- The SmartCard reader is able to hold a secure terminal key to identify each Card reader to the database to show where credit records have been generated.
- The SmartCard reader does not allow any new transactions to be made whilst, data is being transferred to the fraud detection system or remote database.
- The SmartCard reader is capable of creating batches of credit records with incrementing batch numbers.
- The SmartCard reader is capable of holding the previous 20 batches of credit records.

APPL-1002
APPLE INC. / Page 585 of 1892

- Is capable of displaying simple text messages to prompt actions from operators to perform the following tasks:
    1. Authenticate new Card
    2. Apply credit to card
    3. Transfer credit between authenticated Cards
    4. Terminate Card after Credit transfer or discovery of fraudulent use.

Interfaces

- The card reader shall allow interaction to a PC or Point of Sale terminals via either a serial RS232 or other industry standard data transfer interface. The data transferred is encrypted according to a predetermined protocol.
- The card reader system allows remote polling of the system by an external data device, such as the fraud detection system, via modem dial up communications or network connection. This modem can be internal to the card reader system.
- The card reader system initiates communications with the external data device upon command by the program contained in the card reader system.
- The SmartCard reader is dismountable from a host PC if supplied as a separate unit, with minimal requirement for special tools or specialist knowledge by service personnel.
- The card reader is capable of arithmetically deriving SmartCard self identification or SRES based on algorithms held on a mini SmartCard held within the unit.
- The card reader unit is capable of supporting internal readers for plug-in SmartCards conforming to current industry standards.
- The card reader is capable of supporting a main card reader that takes full size cards. This reader has the following characteristics:
    - Push-pull reader with landing contacts;
    - MTBF of 250,000 insertion cycles (minimum);

APPL-1002
APPLE INC. / Page 586 of 1892

- Interface deactivation according to ISO 7816/3;
- Active short circuit protection for the SmartCard;

- The unit is capable of supporting Industry standard protocols, for communication between the SmartCard and the reader, including Asynchronous protocols: T=0, T=1;
- The unit has sufficient memory capabilities to support the requirements of the data capture and transfer routines.
- The unit is capable of supporting Industry standard programming languages that are downloadable over an RS232 interface.
- The card reader system is capable of supporting common point of sale (POS) protocols to accept data transfer from POS systems to allow for updating of the values to the SmartCard.

Security

- The SmartCard reader communications with any external data device are encrypted.
- The SmartCard reader is capable of providing PIN controlled access to all of its functionality including initial access to the screen prompts prior to any form of authentication or credit related actions.
- The SmartCard reader protocols allow no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- The SmartCard reader can detect unauthorised tampering of the SmartCard and causes the SmartCard to cease to function, in this situation.
- The SmartCard reader system software is protected from unauthorised access by either the use of PIN protection only or by the use of PIN protection and a system specific mini SmartCard being read before access to the program is granted.
- Data held on the card reader system is only transferable to other systems or devices upon the entry of security codes or devices as described previously.

APPL-1002
APPLE INC. / Page 587 of 1892

Form factor

- The SmartCard reader is capable of accepting full size SmartCards and/or mini SIM's held within full size card adapters.
- Secondary card readers are provided to accept mini SIM
- The SmartCard reader has an integral display capable of displaying either text or Icons to prompt the operator.
- The SmartCard reader is of a compact size, suitable for co-location with a POS terminal or PC on a customer services desk within a retail store.
- If the SmartCard reader system consists of a PC and card reader, the overall footprint (or size of the system on the desk) does not exceed that of a standard desktop PC. Any screen used in this configuration is not larger than 12" and ideally forms a single unit with the card reader and processor.

Environmental

- The SmartCard reader system supports dual voltage input and is suitable for installation in a number of European countries, with conformance to all relevant environmental requirements e.g. EMC, Noise, Operator ergonomics etc.
- The unit is capable of being hard wired to power supply units (including UPS systems)
- All data, power, telephony communications, and internal SAM connections are capable of being secured in place to prevent unauthorised disconnection of any service.
- The unit can have battery back-up capabilities.

APPL-1002
APPLE INC. / Page 588 of 1892

Handset

Functionality

The Handsets used in this project provide the following functionality:

- Be driven by a SmartCard developed for the Handset so as to provide feedback to a user of the service of the credit remaining on the SmartCard, via the Handset display.
- The Handset display shows the amount of credit available at the start of each call, the end of each call, and by quick access via a hot key sequence. This display is in minutes, viz "Time remaining =? Minutes".
- The Handset is capable of emulating AOC information when none is presented by the network for reference by the SmartCard for charging information purposes.
- Allow calls to predefined numbers held on the card, eg Emergency services and help line number(s) without debiting the credit on the card. The help line number(s) may be allowed a pre-set number of transactions per period at which point additional use is denied until the period is expired.
- The extended menu option which gives access to PIN2 is set to the "OFF" position.
- Allow remote enabling of the Handset and SmartCard upon authenticated request by the network, in combination with user PIN entry.
- Allow remote individual update to the threshold values held in the SmartCard over the network.
- Provide speed dial access to the network operator's voice mail system.
- Call waiting, call swap (in which a call is transferred to another number) and call hold are allowed as long as any outbound call in progress continues to decrement the credit on the SmartCard. The SmartCard allows the barring of calls by Calling Party Category (CPC).

APPL-1002
APPLE INC. / Page 589 of 1892

- The Handset does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2.
- Roaming is not allowed by the Handset.
- The language default, ie the ability to access other network providers original is set to "English".
- The display is capable of displaying an alternating message in the style of "Emergency/Helpline Calls ONLY" and "Operator Name" when credit has expired.
- The display is capable of displaying the operator PLMN code rather than the operator name.
- Line 2 (ie a second line in a call swap) is not supported by the Handset.
- The Handset has the menu functions and associated GSM instruction sets removed or deleted, prior to despatch, for the following call types and menus:
  - Call Transfer;
  - Call forwarding (except Voice Mail);
  - Conference/Multiparty call set up;
  - Roaming facilities;
  - Restricted Dial lists;
  - Sub menu "Bar all incoming calls when roaming";
  - Call divert and sub menus;
  - Select phone line;
  - Call Charge settings;
- The purpose of this is to reduce fraud and costs. Also the space in the Handset that is otherwise used for these functions can be used for other things.
- In addition, the following call types and menus are removed because they cannot be provided by the pre-paid mobile phone system.
  - Change Greeting;

APPL-1002
APPLE INC. / Page 590 of 1892

- All access to SIM memory for:
    - SMS;
    - Phonebook;
    - Capacity add or delete;
    - Copy functions;
    - One touch dialling;
    - Fixed Dialling;
    - Phone Status;
    - Network Selection;
    - Call Meters;

Also:

- The Master Reset or Clear functions are not able to reset or enable any features barred from use.
- Emergency 999/112 calls are allowed without a SmartCard being inserted into the Handset or when credit has expired.
- The Handset is capable of providing a user configurable decrement warning to indicate unit usage, in both visual and audible formats.
- The Handset is capable of providing a "Credit nearing expiry, please recharge" warning to the user in both visual and audible formats.
- The Handset is capable of providing a user warning and also of "tearing down the call" when credit is expired or when a threshold configurable via the card reader or over the radio interface is reached.
- The Handset is capable of providing a "Credit expired, please recharge", warning to the user in both visual and audible formats, and prevent call set up being activated except for emergency and helpline calls.

APPL-1002
APPLE INC. / Page 591 of 1892

- The Handset supports voice calls and the Short Message Service. It supports restricted dialling, phone book, and diverts to voice mail.
- The default Caller line Identifier condition is set to "Present".
- The Handset is capable of being locked to a single network operator and to the SmartCard. These locks are not user addressable under any circumstances.
- The Handset has good standby battery life, in excess of 40 hours and talk time in excess of 90 minutes.
- The Handset supports one number dialling to the network voice mail service.
- The Handset display is easy to read and supports icons as well as text.
- The Handset is capable of supporting calls to pre-determined help line numbers on a toll free basis.
- The Handset manufacturer is able to unlock a SmartCard from its Handset in the repair centre. This is necessary if, for example, the Handset breaks when there is a large amount of credit on the SmartCard.
- The Handset permits Incoming calls when credit has expired.

Interfaces

- The Handset user interface is intuitive to the novice user and presents information in a logical and clear fashion. The use of multiple level menu access for the most common activities is avoided. Integral context sensitive user help is desirable.
- The Handset can support interfaces to data cards for connection from modem or laptop for example, and may have a connection for external power supplies.
- The Handset supports full size SIM cards and ideally contains a SIM release mechanism such that the user does not need to disassemble the Handset or battery to remove the SIM for recharging.
- The SIM does not suffer any harm due to withdrawal of the SIM while the Handset is switched on.

- The SIM to Handset interface supports insertion of the card with a duty cycle in excess of 5000 insertions before any degradation of the interface to the SIM is observed.

Security

- The Handset allows the suppression of access to PIN2 and other Handset menu functions by means of instruction from the SmartCard.
- The access control features are not addressable by the user from the Handset user interface, except for PIN1.
- The Handset has intrinsically good security to prevent unauthorised access to the data transfer between the SmartCard and the Handset.
- The physical design of the Handset is arranged to deter tamper or access to the contacts of the SIM. Ideally any attempt at access to the interior of the Handset leads to the destruction of the Handset.
- Preferably SIM card extenders which enable manipulation of a SIM card by keeping it outside the Handset cannot be with the Handset, when in operation.

Form factor

- The Handset supports full size SIM cards.
- The Handset is of a compact design and subject to evaluation on the basis of appearance, layout, clarity of markings, innovative features, user friendliness, audio quality etc.
- The Handset is of robust construction and provides good ergonomic operation to the user both in call set up and during a call.

Environmental

The Handset is capable of being marked with branding marks, on the front or on the keypad cover as appropriate.

APPL-1002
APPLE INC. / Page 593 of 1892

Accessories

- A full range of accessories including car kits, desk top chargers, desktop hands free kits, data cards (if appropriate) and a range of battery options, can be used with the Handset.
- The Handset is supported by a manufacturer's User Guide, Frequently asked Question and Answer sheets.

Operational requirements

- The network supports advice of charge (AOC) or other suitable systems which can be used to decrement credit held on the prepay SmartCards.
- The network is capable of setting the AOC decrement interval to 10 seconds at delivery and can allow this interval to be configurable over the radio interface to the Handset.
- The network supports remote enabling and disabling of the Handset and SmartCard via authenticated request by the network to the Handset in combination with user PIN entry.
- The network is capable of monitoring the destinations of calls initiated and restrict calls to predefined destinations by National Number Group.
- The network is capable of barring all calls to premium or international destinations.
- The network is capable of preventing call transfer, call forwarding (except to voice mail), conference calls or any non standard or basic call types from being initiated.

The network is capable of allowing Data calls and Short Message Service (SMS) calls on the basis that these are charged at the same rate as voice calls. If this is not possible inbound data and SMS calls only are allowed. The network should be capable of barring these outbound calls if charging on the above basis is not possible.

APPL-1002
APPLE INC. / Page 594 of 1892

Rating and tariff requirements

- A tariff or look up table to be stored in the SmartCard to generate AOC information to the Handset on the basis of flat rate charging is required from the operator.
- The network operator provides the facility to zero rate calls to specified numbers such as helpdesk numbers and emergency calls.
- Over time other tariffs may be introduced, and the network operator is able to support the introduction of new tariff plans via AOC in reasonable time scales.
- Call Detail Records (CDR) produced within the network by use of the present invention are segregated from the operator's other traffic and moved to a secure area for export to the fraud detection system. The frequency of the collation and export of the CDR data shall not exceed 12 hours and may be as frequent as hourly.

APPL-1002
APPLE INC. / Page 595 of 1892

Claims

1. A portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

2. A portable radio communications apparatus as claimed in claim 1 wherein the removable module comprises a SmartCard.

3. A portable radio communications apparatus as claimed in claim 1 or claim 2 wherein the subscriber identification unit comprises a conventional subscriber identification module.

4. A portable radio communications apparatus as claimed in any preceding claim wherein said handset and said removable module are electronically locked such that a particular handset and module pair only function fully together.

5. A portable radio communications apparatus as claimed in claim 4 wherein said handset and said removable module contain information about a secure key that is unique to a particular handset and removable module pair.

6. A portable radio communications apparatus as claimed in any preceding claim which further comprises a timer mechanism adapted to monitor call duration, said timer

APPL-1002
APPLE INC. / Page 596 of 1892

mechanism being adapted to be activated by signals from the handset at the start of a call.

7. A portable radio communications apparatus as claimed in claim 6 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

8. A portable radio communications apparatus as claimed in claim 6 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

9. A communications network comprising at least one portable radio communications apparatus as claimed in any preceding claim.

10. A communications network as claimed in claim 9 comprising a fraud detection system, said fraud detection system comprising database means for storing information about calls made from the handset over the communications network, and information concerning the number of airtime units credited to the electronic purse associated with said portable radio communications apparatus.

11. A communications network as claimed in claim 10 wherein said fraud detection system further comprises a processor adapted to compare the information about calls and the information about electronic purse contents.

12. A removable module suitable for use with a portable radio communications handset said module comprising a rechargeable electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus.

13. A removable module as claimed in claim 12 which contains information about a secure key that is unique to the particular removable module and its handset pair.

APPL-1002
APPLE INC. / Page 597 of 1892

14. A removable module as claimed in claim 12 or claim 13 which comprises a timer mechanism adapted to monitor call duration said timer mechanism being adapted to be activated by signals from the handset at the start of a call.

15. A removable module as claimed in any of claims 12 to claim 14 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

16. A removable module as claimed in any of claims 12 to claim 15 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

17. A recharging system adapted to recharge an electronic purse of a removable module as claimed in any of claims 12 to 16.

18. A recharging system as claimed in claim 17 comprising a reader adapted to read the contents of the electronic purse and means for sending an encrypted update message to the removable module in order to update the electronic purse.

19. A recharging system as claimed in claim 17 or claim 18 comprising at least one database of stored subscriber information and means for comparing the subscriber identification unit with said stored information.

20. A recharging system as claimed in claim 19 comprising at least one local database and at least one remote database.

21. A recharging system as claimed in any of claims 17 to 20 wherein said reader and means for sending an encrypted update message to the removable module are connected to a point of sale apparatus.

22. A recharging system as claimed in claim 21 wherein said reader and said means for sending an encrypted update message to the removable module are electronically locked to the point of sale apparatus.

APPL-1002
APPLE INC. / Page 598 of 1892

23. A portable radio communications handset adapted for use with a removable module as claimed in any of claims 12 to 16, said handset comprising a recess adapted to accept the removable module; and a reading device adapted to determine a content of an electronic purse in the removable module.

24. A portable radio communications handset as claimed in claim 23 wherein said handset is adapted to send a signal to the removable module at the start and end of a call.

25. A portable radio communications handset as claimed in claim 23 or claim 24 wherein said handset contains information about a secure key that is unique to the particular handset and its removable module pair.

26. A method of communicating using a portable radio communications apparatus as claimed in any of claims 1 to 8 said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation.

27. A method as claimed in claim 26 wherein said step of updating the content of the electronic purse involves transmission of encrypted messages between the handset and removable module.

APPL-1002
APPLE INC. / Page 599 of 1892

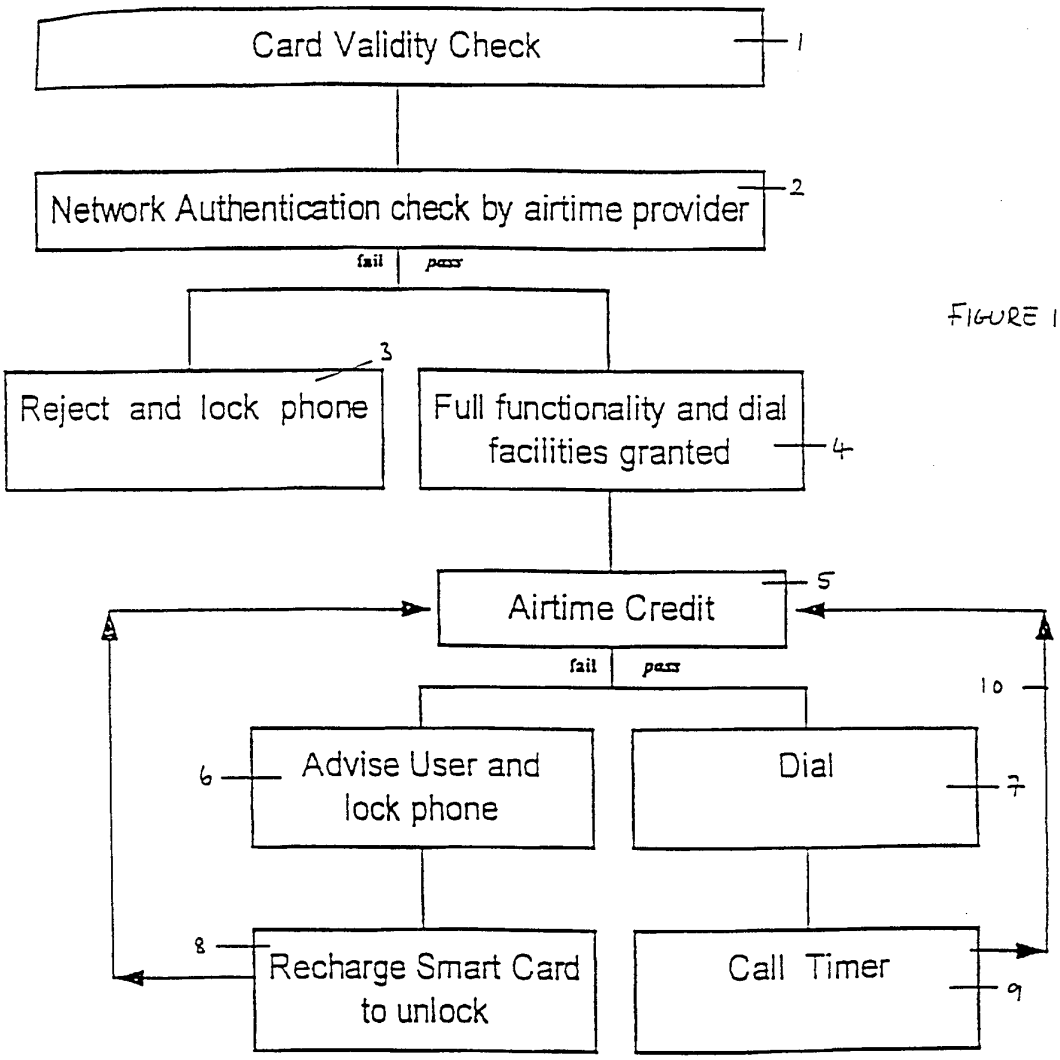

Card Validity Check
1
Network Authentication check by airtime provider
2
fail
pass
3
Reject and lock phone
Full functionality and dial facilities granted
4
Airtime Credit
5
fail
pass
10
6
Advise User and lock phone
Dial
7
8
Recharge Smart Card to unlock
Call Timer
9

FIGURE 1

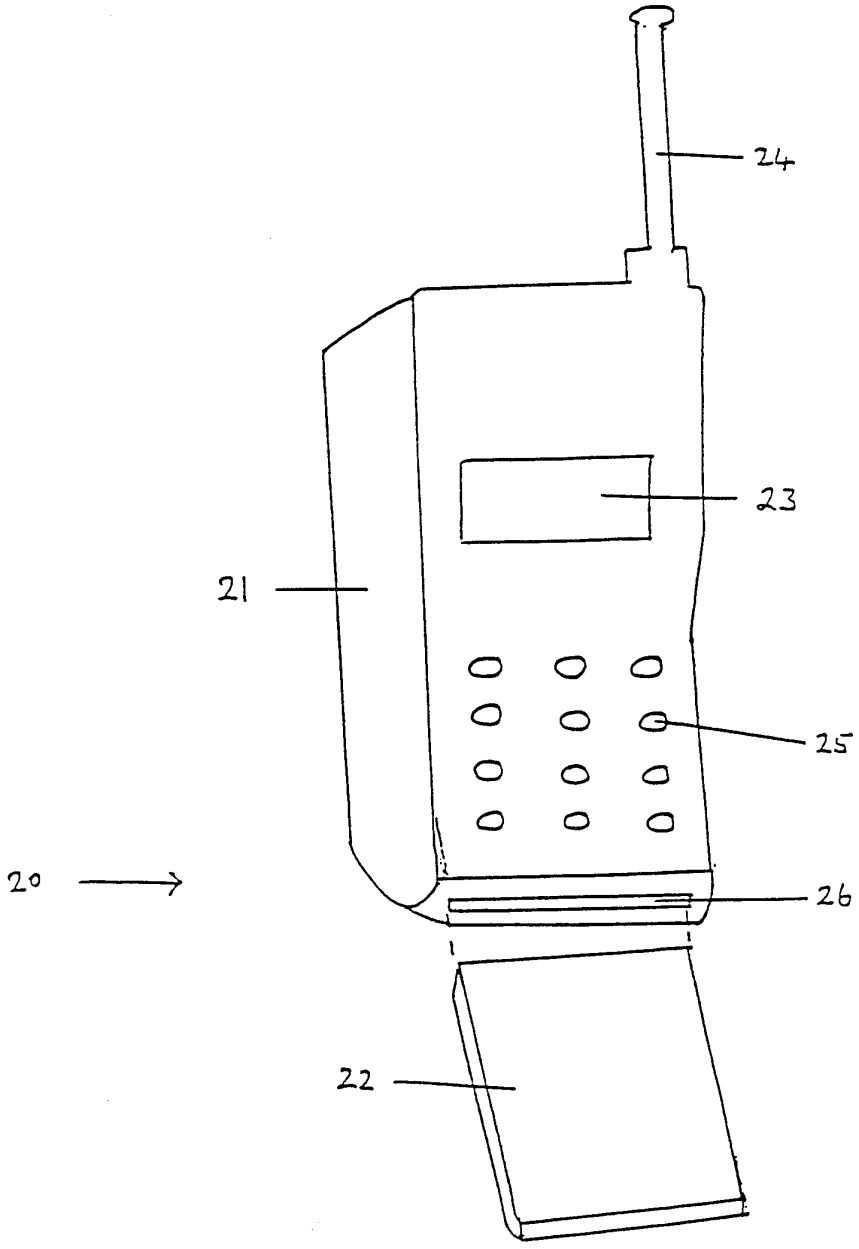


FIGURE 2

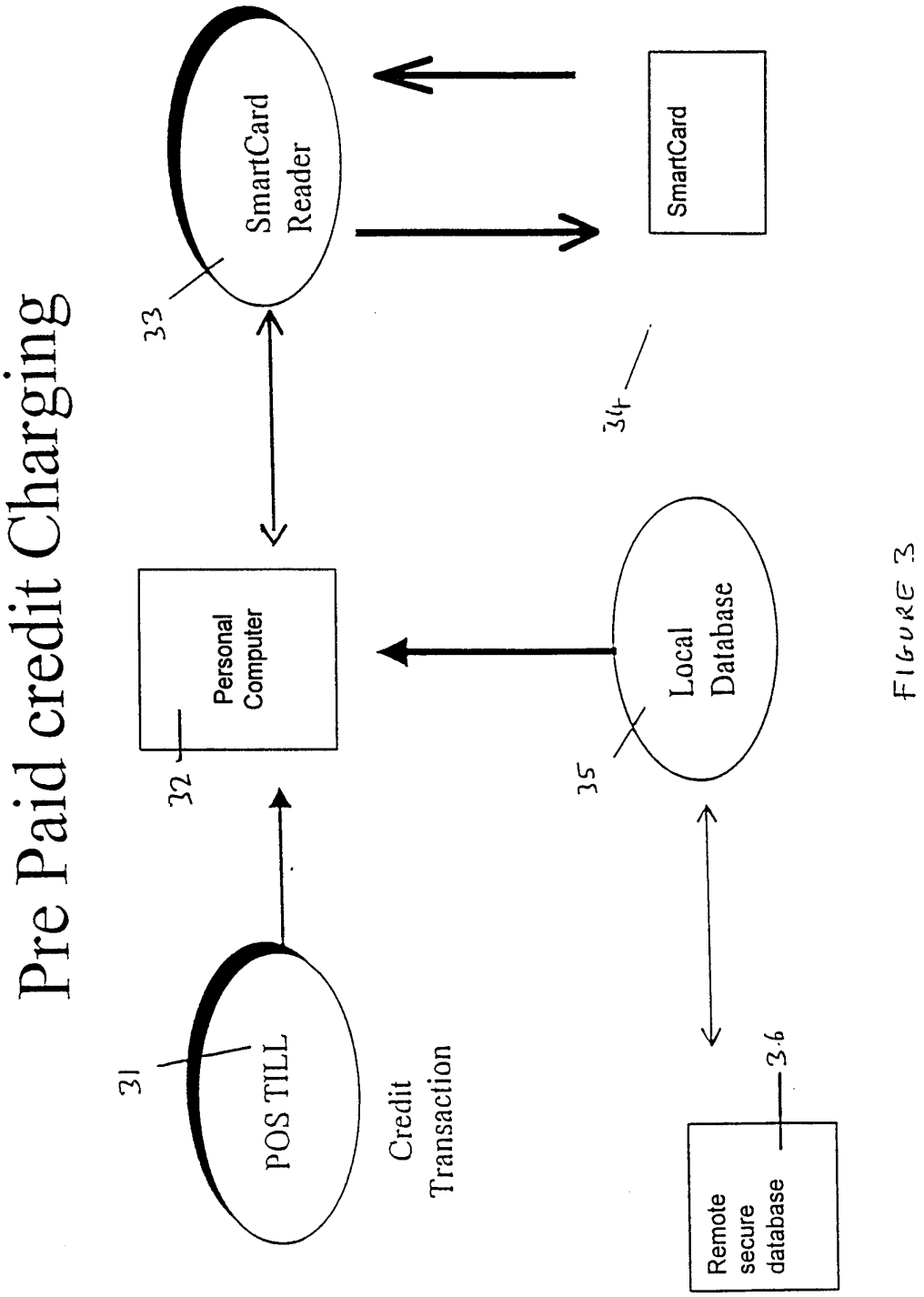


FIGURE 3

APPL-1002
APPLE INC. / Page 602 of 1892

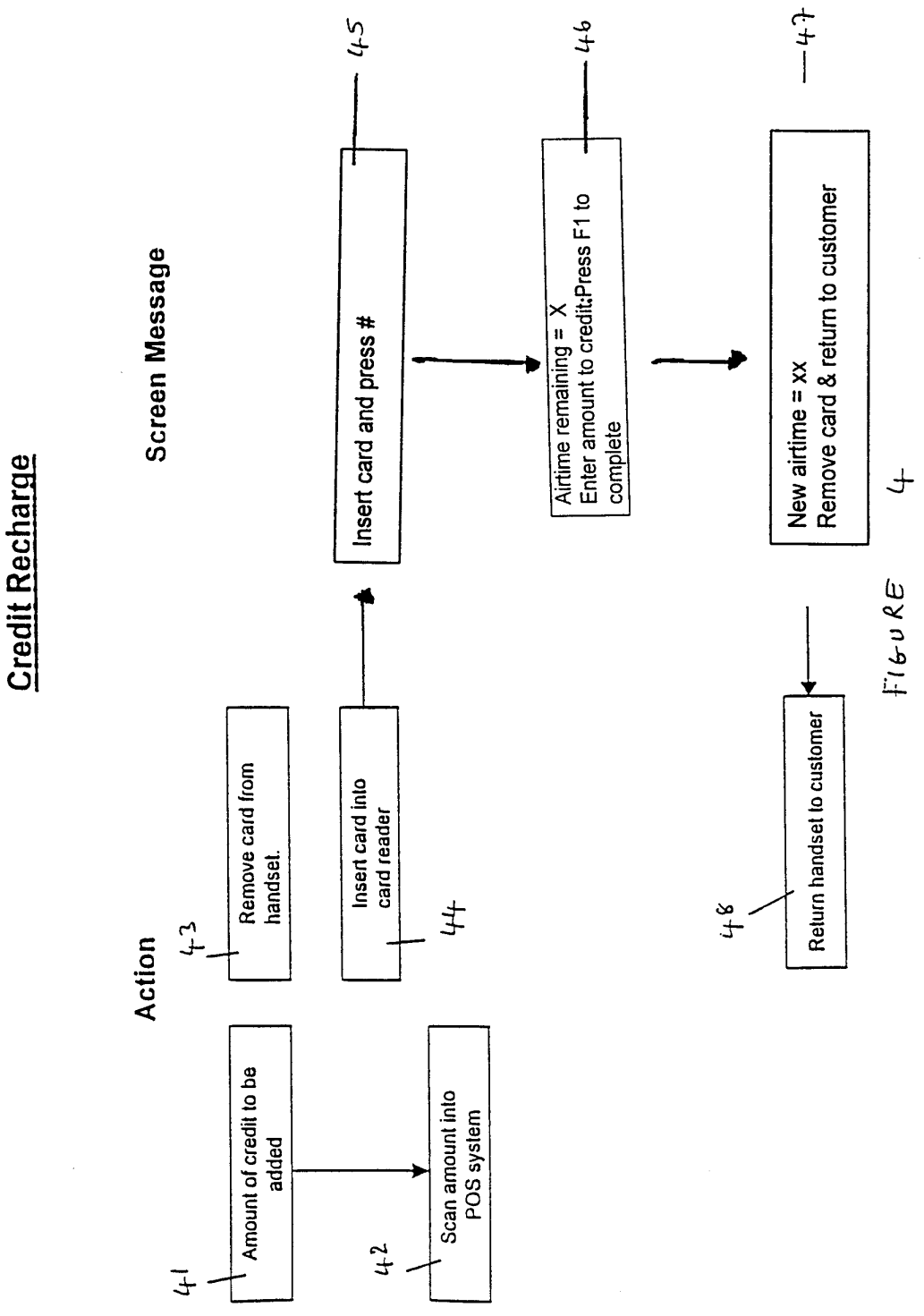

Credit Recharge
Action
Screen Message
Amount of credit to be added
41
Scan amount into POS system
42
Remove card from handset.
43
Insert card into card reader
44
Insert card and press #
45
Airtime remaining = X
Enter amount to credit:Press F1 to complete
46
New airtime = xx
Remove card & return to customer
47
Return handset to customer
48

FIGURE 4

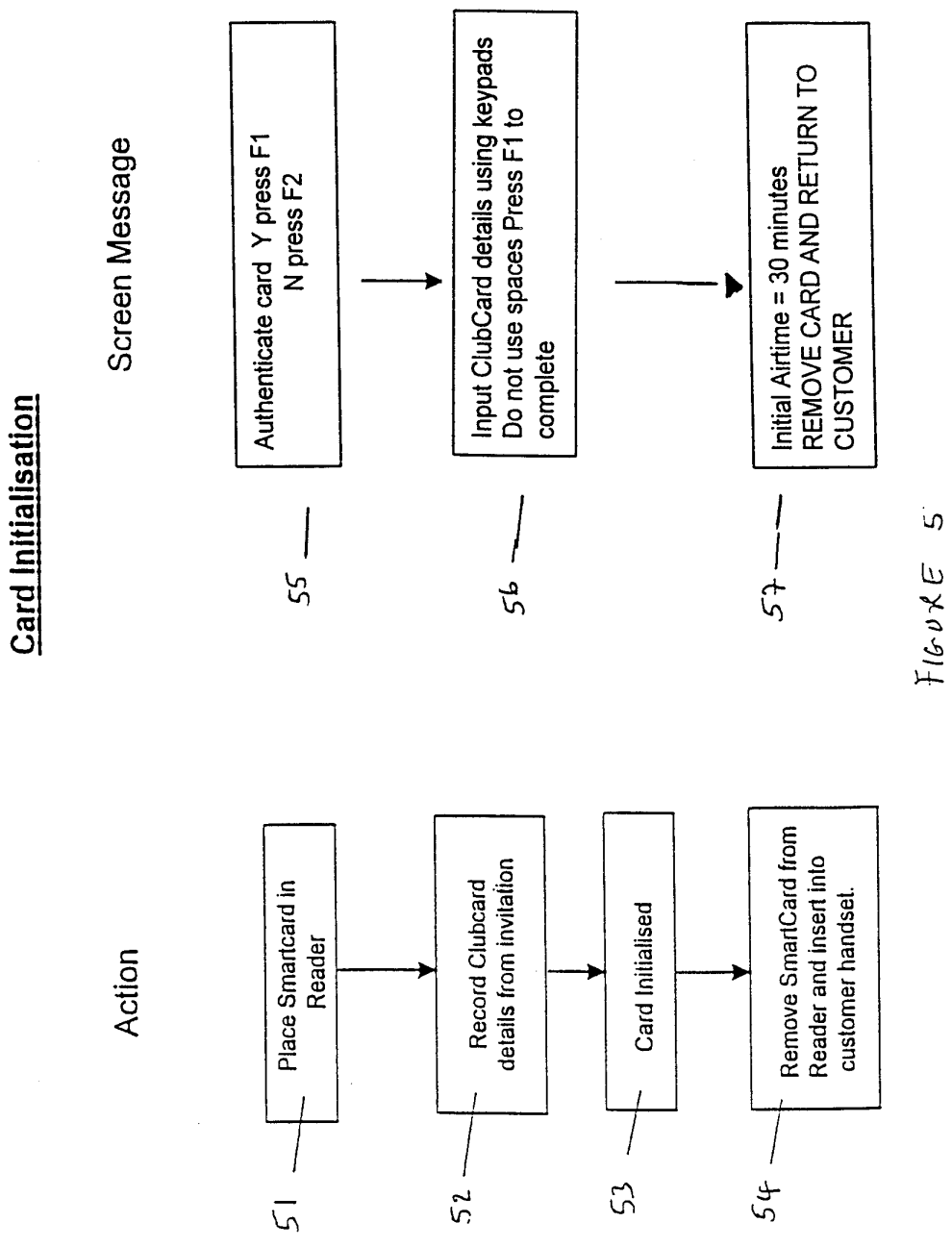

Card Initialisation
Action
Screen Message
Place Smartcard in Reader
Record Clubcard details from invilation
Card Initialised
Remove SmartCard from Reader and insert into customer handset.
Authenticate card Y press F1 N press F2
Input ClubCard details using keypads Do not use spaces Press F1 to complete
Initial Airtime = 30 minutes REMOVE CARD AND RETURN TO CUSTOMER
51
52
53
54
55
56
57

Figure 5

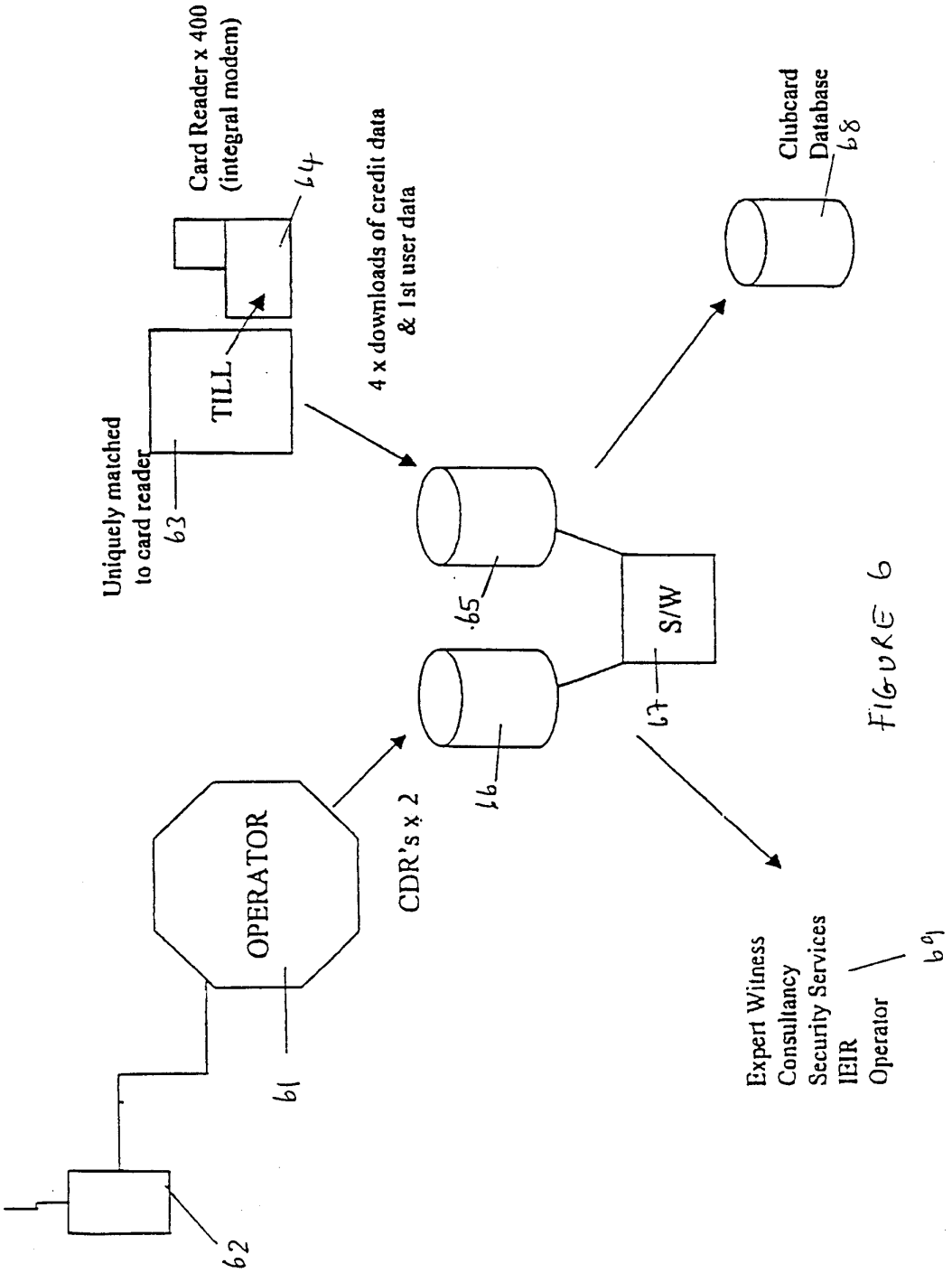

Card Reader x 400
(integral modem)
64
Clubcard
Database
68
4 x downloads of credit data
& 1st user data
TILL
Uniquely matched
to card reader
63
65
S/W
67
OPERATOR
CDR's x 2
66
62
61
Expert Witness
Consultancy
Security Services
IEIR
Operator
69

FIGURE 6

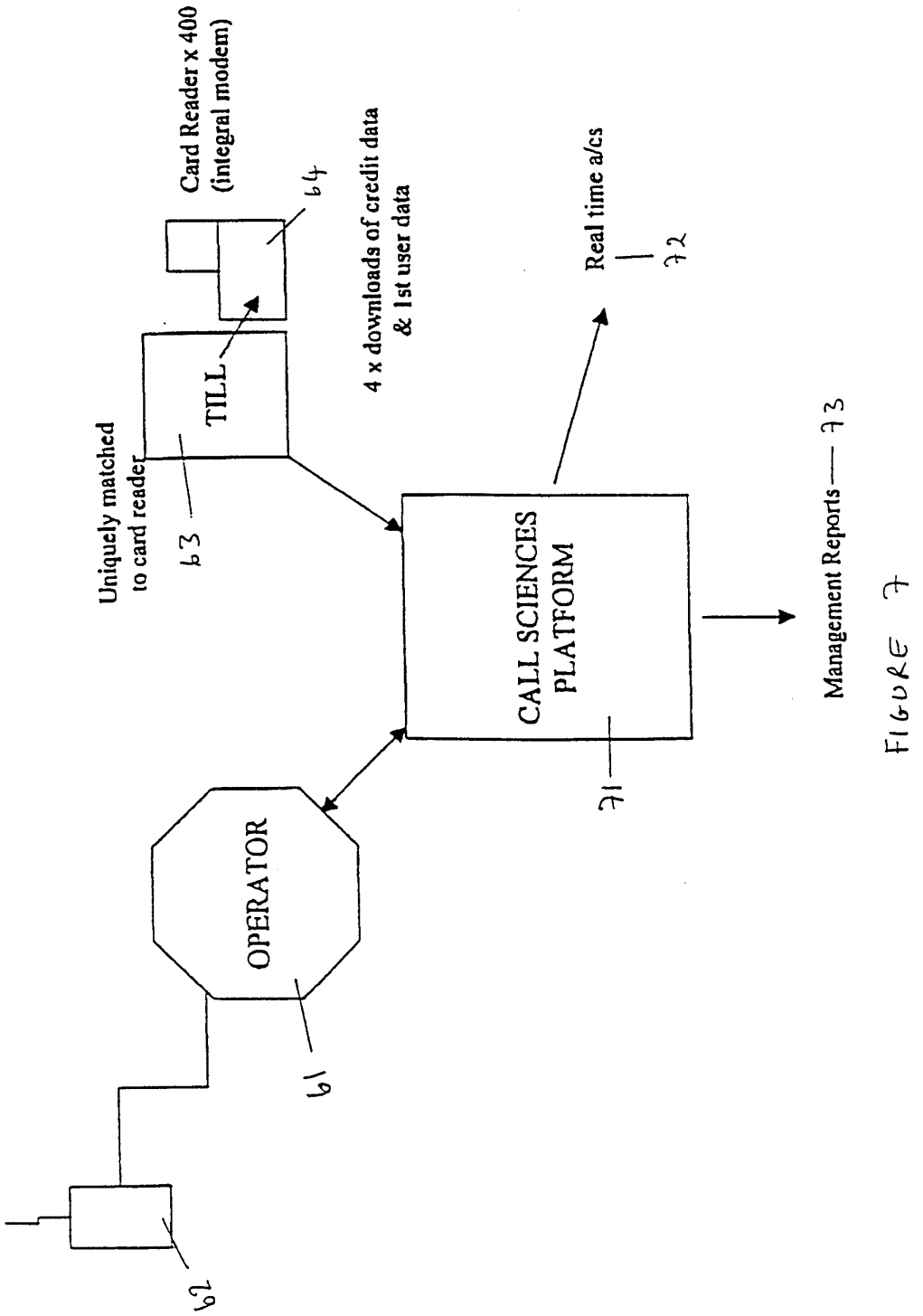

Card Reader x 400
(integral modem)
64
4 x downloads of credit data
& 1st user data
Real time a/cs
72
TILL
Uniquely matched
to card reader
63
CALL SCIENCES
PLATFORM
71
Management Reports
73
OPERATOR
61
62

FIGURE 7

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 98/02729

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00 H04Q7/32

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 H04M H04Q

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	EP 0 790 587 A (PHILIPS ELECTRONICS NV) 20 August 1997	1-3,6-9, 12, 14-17, 23,24, 26,27
A	see column 3, line 26 - column 4, line 21	10
X	WO 95 28062 A (NOKIA TELECOMMUNICATIONS OY) 19 October 1995	1-3,6-9, 12, 14-17, 23,24,26
	see page 3, line 1 - page 4, line 5 see page 8, line 24 - page 10, line 3 see page 11, line 35 - page 13, line 16	
	-/--	

[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
16 December 1998	29/12/1998

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	Neves Appelt, D

1

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

APPL-1002
APPLE INC. / Page 607 of 1892

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 98/02729

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 308 528 A (KARAGOEZLUE IBRAHIM MURAT ;RAMIS HARRY (GB)) 25 June 1997 see abstract see page 4, line 1 - page 6, line 27 see page 11, line 26 - page 12, line 22 see page 14 ---	1-9, 12-17, 23-27
A	US 5 577 109 A (STIMSON CHARLES J ET AL) 19 November 1996 see column 1, line 59 - column 3, line 6 ---	17-22
A	GB 2 267 794 A (CONROY ALAN KILPATRICK) 15 December 1993 cited in the application see page 3 ---	1,2,5,9, 12,13, 17,23, 25,26
A	WO 97 05729 A (TELECOM ITALIA MOBILE S P A ;SENTINELLI MAURO (IT)) 13 February 1997 cited in the application see page 6 - page 7 -----	1-3,6,7, 9,12,14, 15,23,26

1

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

APPL-1002
APPLE INC. / Page 608 of 1892

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/GB 98/02729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0790587 A	20-08-1997	FR 2744822 A	14-08-1997
		CN 1168609 A	24-12-1997
		JP 9233541 A	05-09-1997
WO 9528062 A	19-10-1995	AU 691604 B	21-05-1998
		AU 2216795 A	30-10-1995
		CN 1151240 A	04-06-1997
		EP 0754394 A	22-01-1997
		FI 963996 A	05-12-1996
		JP 10501931 T	17-02-1998
		US 5748720 A	05-05-1998
GB 2308528 A	25-06-1997	NONE	
US 5577109 A	19-11-1996	US 5511114 A	23-04-1996
		AU 2770795 A	04-01-1996
		CA 2192310 A	14-12-1995
		WO 9534161 A	14-12-1995
		US 5721768 A	24-02-1998
GB 2267794 A	15-12-1993	NONE	
WO 9705729 A	13-02-1997	IT RM950521 A	27-01-1997
		AU 6667896 A	26-02-1997
		CA 2227340 A	13-02-1997
		CN 1192308 A	02-09-1998
		CZ 9800233 A	15-07-1998
		EP 0840973 A	13-05-1998
		NO 980341 A	26-03-1998
		PL 324646 A	08-06-1998

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	WO 98/34203
G07F 19/00, H04M 17/00	A1	(43) International Publication Date:	6 August 1998 (06.08.98)

(21) International Application Number: PCT/US98/01391

(22) International Filing Date: 27 January 1998 (27.01.98)

(30) Priority Data:
791,530 30 January 1997 (30.01.97) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 6455 Lusk Boulevard, San Diego, CA 92121 (US).

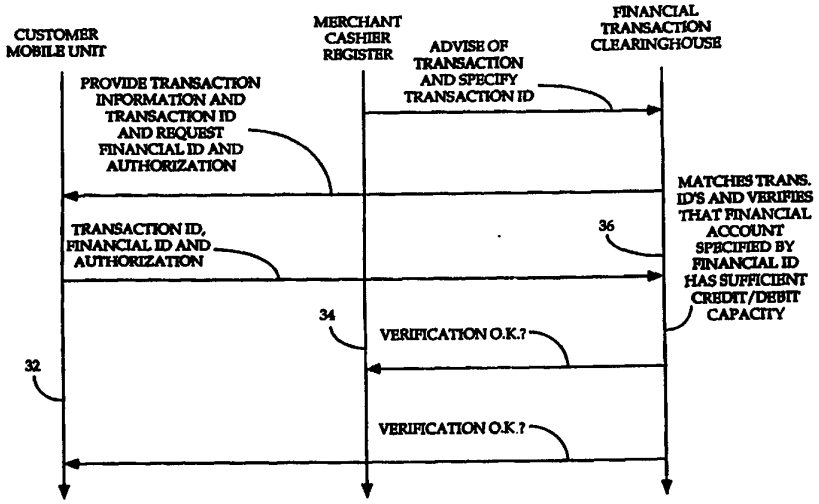
(72) Inventors: JACOBS, Paul, E.; 9075 La Jolla Shores Lane, La Jolla, CA 92037 (US). BELK, Jeffrey, K.; 13967 Arbolitos Drive, Poway, CA 92064 (US).

(74) Agents: OGROD, Gregory, D. et al.; Qualcomm Incorporated, 6455 Lusk Boulevard, San Diego, CA 92121 (US).

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

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT



(57) Abstract

Financial identification codes (ID's) are stored directly within a mobile communications unit (12) such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant, a laptop computer, a dedicated Internet access device, or electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial entities. Storage of financial ID's within such devices allows the various financial ID's of credit (28) and debit accounts (30) of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant (14) or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally reciting the financial ID of a credit or debit account.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT

BACKGROUND OF THE INVENTION

I. Field of the Invention

The invention generally relates to mobile communication units such as mobile telephones and to devices for implementing financial transactions.

II. Description of the Related Art

Consumers increasingly use credit cards, debit cards (such as automated teller machine (ATM) cards), and the like for performing financial transactions with merchants to purchase goods or services. Typically, the consumer provides the credit or debit card to the merchant who runs it through a card scanner to read out a financial identification (ID) associated with the card. The financial ID and the cost of the goods or services are forwarded over a telephone network (such as the public switched telephone network PSTN)) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is sufficient credit or debit capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer.

Among the advantages of this common type of financial transaction is that the consumer need not carry significant amounts of cash for making purchases and may take advantage of any credit granted to him or her. Disadvantages, however, remain. Consumers typically carry numerous credit and debit cards which can be lost or stolen and are often left accidentally with the merchant. Moreover, the financial ID associated with the card is typically recorded on a magnetic strip on the back of the card which can be accidentally erased or otherwise rendered unreadable. Often, purchases are made using credit or debit accounts over the telephone. In such case, the customer must read the financial ID for the account aloud and the merchant must transcribe the financial ID. This is, at best, a tedious and time consuming process and frequent errors occur in reading or transcribing the financial ID's. Moreover, the financial ID may be captured by

unauthorized parties by eavesdropping. Indeed, the party representing itself as the merchant may merely be fraudulently obtaining financial ID's without intending to provide any goods or services. If the purchase is initiated over the Internet, the financial ID is typically conveyed over the Internet via computer transmission signals which again are subject to eavesdropping.

Accordingly, it would be desirable to consolidate all of the financial ID's associated with all of the credit and debit cards of a consumer in a single device not subject to magnetic erasure thereby minimizing the likelihood of misplacing one of the cards and eliminating the risk of having the financial ID accidentally erased. It would also be desirable to consolidate the financial ID's in a device allowing the ID's to be transmitted efficiently such that the financial ID need not be read and transcribed verbally and allowing the financial ID's to be transmitted in an encrypted or otherwise protected form to minimize the risk that the financial ID's may be captured by eavesdropping. Aspects of the invention are directed to solving these and other problems.

To partially address some of these problems, it has been proposed to store the financial ID of a particular credit or debit account on a Smart Card. A Smart Card is similar to a credit card in size and shape but includes electronic circuitry, perhaps in the form of a small microprocessor, for controlling operation of devices receiving the Smart Card and for storing information such as financial ID's. In one possible implementation, the Smart Card is configured to enable telephony operations of the mobile telephone and is also configured to store the financial ID of a single credit or debit account. To effectuate a financial transaction, the Smart Card is removed from the mobile telephone and provided to a merchant for insertion into a Smart Card reader for reading the financial ID therefrom. Although, the use of such a Smart Card has the advantages that the financial ID cannot be easily erased and may be output subject to appropriate encryption, many of the other disadvantages of conventional credit and debit cards remain. For example, depending upon the implementation, a separate Smart Card may be required for each separate credit and debit account and the separate cards are thereby subject to being lost or stolen. Moreover, the consumer may need to terminate a telephone call to allow the Smart Card to be removed from mobile telephone to effectuate the transaction. Finally, because the Smart Card must be inserted into a reader provided by the merchant, no clear advantages are gained for financial transactions conducted over the telephone or using the Internet.

Accordingly, it would be desirable to provide a more effective integration of mobile telephony and financial ID transactions and it is to that end that further aspects of the invention are drawn.

Finally, there is an movement toward enabling the use of digital money for purchase transactions. Digital money constitutes packets of data containing financial ID's defining certain quantities of money that can be transferred from computer to computer. Digital money differs from credit or debit money in that it is not tied to any external real world account. Rather, digital money is the cyberspace equivalent of cash. It would be desirable to provide the aforementioned integration of mobile telephony and financial ID transactions in a manner that enables and facilitates digital money transactions and it is to that end that still further aspects of the invention are drawn.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, financial ID's are stored directly within a mobile communications unit such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant (PDA), a laptop computer, a dedicated Internet access device, or an electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial instruments. Storage of financial ID's within such devices allows the various financial ID's of credit and debit accounts of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally conveying the financial ID of a credit or debit account. Moreover, by storing the financial ID's in the mobile communications unit, the ID's are therefore not as easily subject to inadvertent magnetic erasure as with magnetic strip cards, and the risks associated with misplacing individual credit or debit cards are avoided. The financial ID's may be transmitted in an encrypted form to minimize the risk of unauthorized capture. Almost any form of transaction otherwise conventionally handled with credit or debit accounts or digital money may be performed.

In one embodiment, the invention is implemented within a mobile communications unit by a providing a means for storing a financial

identification code and a means for transmitting the financial identification code to effectuate a financial transaction. A means for receiving a signal representative of a requested financial transaction is also provided along with means for retrieving the financial ID in response to the received request signal. To receive selections from the customer, the mobile communications unit is further provided with a means for providing an indication representative of the financial identification codes to a customer and for requesting selection of one to effectuate transaction; and a means for receiving a selection signal representative of one of the financial identification codes. To receive authorization from the customer to complete a transaction, the mobile communications unit further includes a means for providing an indication of the requested financial transaction to a customer and for requesting approval to effectuate the transaction; a means for receiving an authorization signal representative of whether approval is granted for effectuating the transaction; and a means for transmitting the authorization signal.

Depending upon the implementation, the means for receiving signals and the means for transmitting signals may be an infrared receiver/transmitter, a cellular telephone receiver/transmitter for communicating with a cellular base station, or a mobile telephone receiver/transmitter for communicating with a satellite. Means for encrypting signals prior to transmission and for decrypting received signals may also be employed.

In other embodiments, the invention is implemented as a method.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly throughout and wherein:

FIG. 1 is a block diagram of a financial transaction system configured in accordance with an exemplary implementation of the invention wherein the mobile telephone of a customer has financial ID's stored therein and wherein signals relevant to a purchase transaction are transmitted between the mobile telephone and a merchant cashier register via a cellular telephone system;

FIG. 2 is a flowchart illustrating the steps performed by the system of **FIG. 1** to effectuate a financial transaction in accordance with a first method

wherein a financial ID is transmitted from the mobile telephone to a financial transaction clearinghouse;

FIG. 3 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing a financial ID selection display;

FIG. 4 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing an authorization display;

FIG. 5 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 1**;

FIG. 6 is a timing diagram summarizing, at a high level, a second method wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register;

FIG. 7 is a block diagram of a financial transaction system configured in accordance with a first alternative implementation of the invention wherein signals relevant to the financial transaction are transmitted between the mobile telephone and the merchant cashier register via a satellite-based mobile telephone system;

FIG. 8 is a block diagram of a financial transaction system configured in accordance with a second alternative implementation wherein signals relevant to the transaction are transmitted between the mobile telephone and the merchant cashier register via infrared signals;

FIG. 9 is a block diagram of a financial transaction system configured in accordance with a third alternative implementation and wherein signals relevant to a transaction initiated during a telephone call are transmitted between the mobile telephone and the merchant cashier register via a cellular telephone system;

FIG. 10 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a first method wherein a credit or debit account is accessed;

FIG. 11 is a timing diagram illustrating, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a second method wherein digital money is transferred;

FIG. 12 is a block diagram of a financial transaction system configured in accordance with a fourth alternative implementation of the invention wherein signals relevant to a transaction initiated via the Internet are transmitted between the mobile telephone and a merchant computer via a cellular telephone system connected to the Internet;

FIG. 13 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 12** to effectuate a financial transaction in