

MOBILE PHONE AS A POINT OF SALE (POS) DEVICE

RELATED APPLICATION

[0001] This application is a continuation-in-part of US Patent Application Serial No. 11/503,903 filed August 15, 2006, which in turn claims priority from U. S. Provisional Application No. 60/733,266, filed on November 4, 2005, all incorporated herein by reference.

FIELD OF INVENTION

[0002] The present invention relates generally to the enablement of wireless communication devices as transaction gateways. More particularly, the present invention relates to a system and method for enabling a wireless handset as a point-of-sale (POS) device.

BACKGROUND OF INVENTION

[0003] With the explosion of wireless phone access and usage, cellular phone service is fast becoming more and more available in developing countries where landline infrastructures are generally considered insufficient. Consequently, mobile service providers or operators are finding captive consumers in these countries for mobile phone services, particularly pre-paid phone cards.

[0004] The following prior art patent represent the state of the art for the transfer of digital data to a mobile device, and is hereby incorporated by reference:

[0005] U. S. Patent No. 6,714,797 to Rautila discloses a system, method and computer program for ordering, paying for and downloading digital products to a mobile device. The mobile device accesses electronic shop server web sites that contain digital products for sale and hotspot network locations where these digital products may be downloaded to the mobile device via the

short range transceiver located in the mobile device. Using the system, method and computer program disclosed therein, a user of a mobile device may download large amounts of digital data without incurring telephone or cellular phone charges.

[0006] However, a problem with the above-mentioned prior art system is its inflexibility. From the mobile operator's perspective, for example, such existing cellular applications do not allow for the delivery of digital content to pre paid, post-paid or third party paid mobile phone subscribers, so prevalent and growing in developing countries. Such current implementations of pre-payment, post-payment or third-party bill payment systems lack flexibility, ease of implementation and responsiveness.

SUMMARY OF INVENTION

[0007] The present invention satisfies, to a great extent, the foregoing and other needs not currently satisfied by existing mobile commercial applications.

[0008] This result is accomplished, in an exemplary embodiment, by a system and method that activates the delivery of digital content and/or the pre-payment, post-payment or third-party bill payment of mobile operator and/or third party goods or services using a wireless communication device as a transaction gateway by one or more retailers or mobile operators. For ease of discussion, the term, "retailer", is used to refer to one or more mobile operator agents and/or independent retailers.

[0009] Using a mobile based application protocol, such as, but not limited to, short message service (SMS), wireless application protocol (WAP), the Java 2 Platform Micro Edition (J2ME), SIM Application Toolkit (STK), BREW, etc., the wireless communication device communicates with or browses an electronic mobile commerce server. The mobile commerce (M-Commerce) server provides access to a range of electronic or digital products supplied from the mobile

operator and/or one or more third party providers available for purchase by the mobile phone service subscriber through one or more independent retailers and/or mobile operator agents. These third party providers may take the form of one or more specialized servers, such as a SMS center, a WAP gateway or a J2ME server, which operates in communication with the m-Commerce server.

[0010] In one aspect of the present invention, a value-added services (VAS) server is configured to provide enhanced digital content and/or enhanced services to the purchasing mobile phone service subscriber. Each enhanced digital content and/or service is packagable as a VAS content purchase of one or more enhanced services for pre-paid and post-paid mobile phone subscribers. In addition, each enhanced service is configurable to interoperate with one or more electronic platforms, such as a color ring tone platform, a post-paid billing platform, a vendor content delivery platform, and the like.

[0011] The VAS content or enhanced services include ring tones, music, virtual calling cards, and short message service (SMS) alert subscription services.

[0012] For instance, the VAS server preferably includes the provisioning of content directed to a variety of ring tones, logos, picture messages, video, music, games and other content. In this regard, the VAS server allows for content selection from an available list of content advertised by a mobile operator and/or retailer. The VAS server may also provide a subscription to a color ring tone service, allowing for song selection from an available list of musical content advertised by a mobile operator and/or retailer. Further, short message service (SMS) alert subscription services for news, sports, horoscope and such information may also be made available from the VAS server for ultimate pass through to the subscriber user. In addition, in instances where a mobile operator or third party provider employs its own calling card platform, the VAS server is

configurable to provide virtual calling card or VAS card personal identification numbers (PINs) for use on the operator's or third party provider's platform.

[0013] Notably, these VAS server content or enhanced services are preferably modular in that each content/service may be enabled or disabled as desired on an individual basis.

[0014] In a preferred embodiment, the VAS server incorporates a content management system, which manages the server's operational functions. The content management system does not need to store or deliver VAS content to the target mobile phone service subscriber. It is integrated with the appropriate vendor's content delivery platform, which is responsible for the actual service provisioning and/or content delivery to the target mobile phone service subscriber. The VAS server, through communication with the M-Commerce server, facilitates access of a desired vendor's content and/or enhanced services to one or more retailers, and triggers the vendor's content delivery platform to send the content or enhanced services to the target subscriber. In this regard, the content management system assists in providing several functions, such as: the generation of centralized VAS codes; validation of VAS codes, management of VAS prices by retailer group or geographical region; management of VAS prices by retailer margin definition and calculation by retailer group or geographical region; availability of VAS by retailer group or geographical region; promotion of specific VAS by retailer group or geographical region; and other reporting.

[0015] Alternatively, rather than the content management system being connected to one or more separate vendor content delivery platforms such that the content is delivered by these platforms remotely, content may be stored locally on the content management system such that the content is delivered from the VAS server via the content management system directly.

[0016] The M-Commerce server also manages the interoperability of the VAS server with other platforms, such as the mobile operator billing system, the content provider VAS platform, etc. In a preferred embodiment, each retailer is equipped with electronic wallet accounts, which has pre-paid credits. When a purchase is requested, the value is deducted from the retailer's pre-paid e-wallet account. The retailer's e-wallet account also operates with a credit whereby retailers may settle accounts with mobile operators periodically.

[0017] In another aspect of the present invention regarding a logical view of the server configuration, the system of the present invention comprises an application layer, a middleware layer and an interface layer. The application layer performs all of the transaction processing functions, and manages integration with operator network entities, third party provider network entities and the application layer modules and sub-systems. The middleware layer standardizes and manages communications between all external network entities and the modules and sub-systems of the application layer. The interface layer comprises one or more interface modules written for each specific target platform, for example. Each interface module implements a specific communications protocol, facilitating plug-and-play integration with third party provider network entities and mobile operator network entities.

[0018] More specifically, the application layer comprises three modules: an m-Commerce server, and e-Wallet server and a VAS server. Each of the three server modules are composed of sub-systems. For example, the m-Commerce server module comprises four sub-systems or four main functional blocks: agent registration and management; parsing & end-to-end transaction management; transaction log, audit and reporting; and settlement and reconciliation. The e-Wallet server module comprises three sub-systems: e-Wallet transaction management; e-Wallet stored value; and agent authentication and security. And the VAS server module is composed of

five sub-systems: VAS transaction management; content mapping; retailer verification; VAS pricing and retailer commission; and PIN database. Each of these sub-systems is configured to perform intended functions required of the respective server module.

[0019] The middleware layer is best described by the complexity of core functions it manages, such as multi-threading management queuing, message delivery and recovery, system monitoring, data collection, transaction management and logging, and the like. It lies between the application layer and the interface layer.

[0020] The interface layer is composed of a plurality of interface modules that incorporate features designed to manage the transaction load on the target network entity and simplify integration of third party network entities or mobile operator network entities. In this embodiment, the interface modules comprise a SMSC interface; a WAP interface, a content interface; a color ring tone interface; an information alert interface; and a postpaid interface, each of which preferably corresponds to a respective platform or network entity it supports.

[0021] In yet another aspect of the present invention, a third party billing server is configured to facilitate delivery of a wide range of electronic or digital products and services provided by one or more third party providers. These products and services may include remote purchases, bill payments, currency collection, electronic PINs, point to point payments, account inquiries and the like. Furthermore, a subscription service or wireless device is not necessarily required by the user. Each of these products and services are configurable to interoperate with one or more third party provider platforms, such as a utility company platform, credit card company platform, financial institution platform, or any other merchant / retailer / third party provider platform and the like. Notably, any of these electronic or digital products and services is preferably modular in that each product/service may be enable or disabled as desired on an individual basis.

[0022] In a preferred embodiment, the third party billing server, through communication with the M-Commerce server, facilitates delivery of a desired third party provider's content and/or services to one or more retailers or merchants, and triggers the third party provider's platform to send the content or service to the target user.

[0023] In addition, the application layer of this aspect of the present invention comprises an M-Commerce server, an e-Wallet server and a third party billing server. The M-Commerce server and e-Wallet server modules are composed of subsystems as earlier described. The sub-systems of the third party billing server includes: third party transaction management, retailer verification, PIN database and third party retailer commission. Each of these sub-systems is configured to perform intended functions required of the respective server module. The middleware and interface layers are as earlier described, except that in this aspect of the invention the interface modules include a SMSC interface; a WAP interface; any number of merchant or third party provider interfaces such as one from an electric company, a gas company, credit card company, water company and the like, each of which preferably corresponds to a respective platform or network entity it supports.

[0024] The configuration of the application layer, middleware layer and interface layer modules and sub-systems provision a system and method for enabling a wireless communication device as a point-of-sale device that is highly scalable, robust and secure. As to scalability, the modules are designed to act as 'stand-alone' processes that communicate with other modules, preferably via XML messages over TCP/IP sockets. The modules may reside on the same server, or be distributed over a network or a cluster. Modules are also configurable to send messages to multiple modules, thus allowing load balancing throughout the three architecture layers. Applications may also be distributed across multiple servers. In addition, multiple instances of

the modules and interfaces may be configurable in fail-over mode across multiple stand-alone or clustered servers.

[0025] As to robustness, each module provides shutdown and re-start procedures that allow pending transactions to be processed if possible. In addition, if a module sends a message to another module, and that transaction fails, it will automatically attempt to re-send the message to a redundant module. Also, if an attempt to re-send the transaction also fails – such as in the case of absolute failure – then the message is spooled to disk, and an internal monitoring thread will attempt to re-send the message at a later time.

[0026] As to security, secure communications throughout the architecture of the present invention ensures that sensitive data is not compromised. Module-to-module communications are preferably encrypted to ensure message integrity. Supported encryption algorithms include 3DES, Blowfish, AES, SSL and the like. Supported hashing algorithms (for message integrity checking) include MD5, SHA1 and the like. Links with external entities are also preferably encrypted with any of the above software based algorithms. Hardware based encryption modules (HSM) may be integrated to encrypt transactions with external entities.

[0027] There has thus been outlined, rather broadly, the more important features of the invention in order that the detailed description thereof that follows may be better understood, and in order that the present contribution to the art may be better appreciated. There are, of course, additional features of the invention that will be described further hereinafter.

[0028] In this respect, before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried

out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0029] As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may be readily utilized as a basis for the designing of other structures, methods and systems for carrying out the several purposes of the present invention. It is important, therefore, that equivalent constructions insofar as they do not depart from the spirit and scope of the present invention, are included in the present invention.

[0030] What is more, the detailed description that follows may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are the means used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art.

[0031] A procedure is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, entities, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0032] Further, the manipulations performed are often referred to in terms, such as providing, inputting, confirming or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present

invention; the operations are machine operations. Useful machines for performing the operation of the present invention include general purpose digital computers or similar devices.

[0033] The present invention also relates to a system for performing these operations. This system may be specially constructed for the required purpose or its may comprise a general purpose computer as selectively activated or reconfigured by a computer program stored in a computer. The procedures presented herein are not inherently related to a particular computer or other system or apparatus. Various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct more specialized system/apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

[0034] For a better understanding of the invention, its operating advantages and the aims attained by its uses, references should be had to the accompanying drawings and descriptive matter which illustrate preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGSEMBODIMENTS

[0035] Fig. 1 is a physical view of the server configuration of a system for enabling a wireless communication device as a point-of-service device, in accordance with a preferred embodiment of the present invention.

[0036] Fig. 2 is a logical view of the server configuration of the system of Fig. 1.

[0037] Fig. 3 is a diagram of the middleware of Fig. 2.

[0038] Figs. 4A and 4B show a flowchart of a post-paid bill pay transaction using the system of Figs. 1 and 2.

[0039] Figs. 5A and 5B show a flowchart of a content purchase transaction in the form of a ring tone using the system of Figs. 1 and 2.

[0040] Figs. 6A and 6B show a flowchart of an enhanced service subscription purchase transaction in the form of a color ring tone using the system of Figs. 1 and 2.

[0041] Figs. 7A and 7B show a flowchart of an enhanced service subscription transaction in the form of a color ring tone song purchase transaction using the system of Figs. 1 and 2.

[0042] Figs. 8A and 8B show a flowchart of an enhanced service purchase transaction in the form of a virtual calling card using the system of Figs. 1 and 2.

[0043] Figs. 9A and 9B show a flowchart of an enhanced service subscription transaction in the form of an alert service using the system of Figs. 1 and 2.

[0044] Fig. 10 is a physical view of the server configuration of a system for enabling a wireless communication device as a point-of-service device, in accordance with an alternative embodiment of the present invention.

[0045] Fig. 11 is a logical view of the server configuration of the system of Fig. 10.

[0046] Fig. 12 illustrates a flowchart of an exemplary third party bill payment transaction using the system of the embodiment of Figs. 10 and 11.

[0047] Fig. 13 illustrates a flowchart of another exemplary third party bill payment transaction using the system of the embodiment of Figs. 10 and 11.

[0048] Fig. 14 illustrates a flowchart of an exemplary third party disbursement transaction using the system of the embodiment of Figs. 10 and 11.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0049] Referring now to the figures, wherein like reference numbers indicate like elements, in Fig. 1 there is shown an exemplary embodiment of a system for enabling a wireless communication device as a point-of-sale (POS) device.

[0050] As depicted in a physical view of the system's server configuration, the wireless communication device 12, such as a mobile phone, is used by a retailer or mobile operator 10 as a POS device to access an electronic mobile commerce (M-Commerce) server 16 through a 2.5G, third generation (3G) or later global system for mobile communication (GSM) 14. Mobile operator network entities, such as a SMS center, WAP gateway and a J2ME server, are preferably collocated at 14 and communicate with the M-Commerce server 16 through SMS center and WAP gateway interfaces. The M-Commerce server 16 communicates via a middleware layer to an e-Wallet server 22, pre-paid top-up distribution server 20 and a VAS server 18. The VAS server 18 in turn communicates through interfaces with target platforms 23, 17, 19, 17, which may be owned by one or more third party providers or mobile operators.

[0051] For ease of discussion, retailer 10 is used to refer interchangeably to one or more mobile operator agents and/or independent retailers.

[0052] The M-Commerce server 16 provides a menu of one or more electronic or digital products. These products may be supplied by the retailer, the mobile operator itself, or from one or more content providers represented as value-added services (VAS) content and/or enhanced services, which operate in tandem with a mobile operator's system(s).

[0053] More specifically, the M-Commerce server 16 provides the operational logic to manage an end-to-end M-Commerce transaction, including but not limited to: an interface logic - such as wireless application protocol (WAP), short message service (SMS), Java 2 Platform Micro Edition (J2ME), Java Micro Edition (JME), SIM Application Toolkit (STK), etc. - for integration with a mobile operator's access channels; parsing logic to receive and process transactions from various access devices using the above-mentioned interface logic; a transaction management logic to control performance of desired transactions, such as content purchase transactions,

enhanced service subscription transactions, enhanced service purchase transactions and the like; integration capabilities to facilitate integration with one or more sub-systems, such as the VAS server 18, pre-paid top-up distribution server 20 and e-wallet server 22; and other operational support capabilities including but not limited to configuration, reporting, auditing, etc.

[0054] The VAS server 18 provides the operational logic to manage the transactional processing that occurs between the retailer 10 and any third party provider platform, such as the color ring tone platform 17, vendor content delivery platform 21 and information alert platform 23 depicted in Fig. 1. The VAS server also manages the transactional processing that occurs between the retailer 10 and the mobile operator's platform, such as the post-paid billing platform 19.

[0055] More specifically, the VAS server 18 provides operational logic, which includes but is not limited to: an interface logic for integration with a mobile operator's access channels and a third party provider platform; a transaction management logic to control performance of desired transactions, such as content purchase transactions, enhanced service subscription transactions, enhanced service purchase transactions and the like; and other operational support capabilities including but not limited to mapping and validation of mobile operator content ID, authenticating authority for retailers to sell specified content and/or enhanced services, establishing retail prices and commissions, system configuration, reporting, auditing, etc.

[0056] The color ring tone platform 17, which preferably exists in the network of a mobile operator or third party provider, is hardware and software used to house or store the audio files of the color ring tone content. In the provisioning of color ring tone services, the color ring tone platform 17 is interconnected to a mobile operator's switching infrastructure to substitute the audio file of a selected song for another network ring tone in a subscriber's handset.

[0057] The post-paid billing platform 19, which preferably exists in the network of a mobile operator or third party provider, is hardware and software used to capture call records, generate accounts and track payments for post-paid services.

[0058] The vendor content delivery platform 21, which preferably exists in the network of a mobile operator or third party provider, is hardware and software used to house or store digital content. In the provisioning of digital content, the vendor content delivery platform 21 is interconnected to a mobile operator's switching infrastructure to deliver selected content to a subscriber's handset.

[0059] The information alert platform 23, which preferably exists in the network of a mobile operator or third party provider, is hardware and software used to house or store information and data. In the provisioning of alert subscription services, the information alert platform 23 is interconnected to a mobile operator's switching infrastructure to deliver selected subscription information alerts to a subscriber's handset.

[0060] A preferred embodiment of a logical view of the server configuration of the system of the present invention is shown in Fig. 2. The application architecture performs all of the transaction processing functions, and manages integration amongst and between the server modules 16, 18, 22, its sub-systems, the middleware 15, the various third party network platforms 17, 21, 23, and any mobile operator network entities, such as the postpaid billing platform 19, the SMS center 24, the WAP gateway(s) 25 and the J2ME server(s) 26. The application architecture also manages the back-end administration, reporting and monitoring infrastructure.

[0061] Preferably, the middleware layer 15, and the SMS center and WAP interfaces 24a, 25a are collocated with the M-Commerce server 16. Similarly, the middleware layer 15 and the

interfaces 21a, 17a, 23a, 19a are preferably collocated with the VAS server 18. Finally, the middleware layer 15, in the absence of any interface components, is collocated with the e-Wallet server 22.

[0062] As depicted in Fig. 1, the M-Commerce server 16, e-Wallet server 22 and VAS server 18 may be viewed as the three primary modules developed to support a VAS content and enhanced services application. This is the application layer. These modules contain the business logic for each particular solution, and are separated into discrete functional blocks, which interact with each other and with the middleware and interface layers.

[0063] For example, the M-Commerce server 16 includes four functional blocks; namely, an agent registration and management block 16a, a parsing and end-to-end transaction management block 16b, a transaction log, audit, reporting block 16c, and a settlement and reconciliation block 16d.

[0064] The agent registration and management block 16a provides the business logic to register and manage an agent's (i.e. retailer's) virtual account. Block 16a also includes, but is not limited to, the operational logic that: performs the agent registration function, and allocates the agent against a group of agents. Preferably, for example, each retailer has parameters that govern their characteristics and operations, such as sales commissions, maximum and minimum e-wallet balance caps, maximum transaction volume caps, maximum transaction value caps, products they are authorized to sell, and the like. An operator generally has a set number of combinations of these parameters, such as three or four commission structures. For ease of management, the agent registration and management block 16a enables the operator to create one or more groups where each group represents one or more sets of parameter combinations. Thus, when registering a retailer, the operator may assign a retailer to a group, and the retailer automatically adopts the

characteristics for that group. In this way, the retailer registration process is streamlined (i.e. less data to enter for each specific retailer) and wholesale changes to a large number of retailers may be implemented by changing the group parameters.

[0065] The parsing and end-to-end transaction management block 16b provides the business logic to manage the end-to-end transaction flow and interaction between all three modules 16, 22, 18. Block 16b also includes, but is not limited to: an interface logic to integrate with the mobile operator or third party provider access channels, such as SMSC 24, Wireless Application Protocol (WAP), etc.; a parsing logic to receive and process transactions from the various access devices using the protocols associated with one or more source platforms such as SMSC 24, WAP gateway 25, J2ME server 26, etc.; a decryption algorithm to decrypt incoming messages; a transaction management logic to control the end-to-end transaction flows; software for integration with the other modules, such as the e-Wallet server 22 and the VAS server 18; and software to provide all of the operational support functions including, but not limited to, system configuration, reporting, auditing, etc.

[0066] The transaction log, audit and reporting block 16c provides the business logic to capture and store the end-to-end transaction data. This block 16c also includes, but is not limited to: transaction data logging functions for end-to-end transactions; audition functions; and reporting functions.

[0067] The settlement and reconciliation block 16d provides the business logic to calculate transaction fees and commissions for all parties to the transaction in real time. It supports fixed fee or variable percentage transaction amounts, or both.

[0068] The e-Wallet server 22 comprises three main functional blocks; namely, the e-Wallet transaction management block 22a, the e-Wallet stored value block 22b, and the agent

authentication and security block 22c. The e-Wallet transaction management block 22a provides the business logic to manage the interaction with the agent's or retailer's virtual account. The capabilities of this block 22a include, but are not limited to: routing transactions from/to the M-Commerce server 16 and the VAS server 18; transaction data logging for e-Wallet auditing and reporting.

[0069] The e-Wallet stored value block 22b provides the operational logic to manage the intra-actions of an agent's or retailer's virtual account. The capabilities of this block 22b includes, but are not limited to: storing current e-Wallet account balances, status and information; responding to balance inquiries from the M-Commerce and VAS servers 16, 18; reserving funds while a transaction is being processed by either of the M-Commerce and VAS servers 16, 18; and committing funds to or from the virtual account once a transaction is successfully completed.

[0070] For ease of discussion herein, it is assumed that a retailer's electronic wallet has sufficient credits for the desired transaction. Alternatively and/or optionally, the retailer 10 may use non-electronic mechanisms to effect a mobile phone related sales transaction, such as selecting the desired mobile phone-related product from a local/remote catalog.

[0071] The agent authentication and security functional block 22c provides the business logic for managing authentication and security functions. The capabilities of block 22c include, but are not limited to: storing an agent's or retailer's M-Commerce server identification number (M-PIN) in a secure manner; and responding to agent/retailer authentication requests from the other modules 16, 18, including validation of the M-PIN.

[0072] The last of the three primary modules depicted in Fig. 2 is the VAS server 18, which comprises five main functional blocks; namely, a VAS transaction management block 18a, a

content mapping block 18b, a retailer verification block 18c, a VAS pricing and retailer commission block 18d, and a PIN database block 18e.

[0073] The VAS server transaction management block 18a provides the business logic to manage the transaction aspects of delivery of the content or enhanced service. The capabilities of block 18a include, but are not limited to: routing transactions from/to the M-Commerce and e-Wallet servers 16, 22; routing transactions from/to the interfaces 21a, 17a, 23a, 19a for the platforms 21, 17, 23, 19, respectively; and transaction data logging for VAS service auditing and reporting.

[0074] The content ID mapping block 18b provides the business logic to manage the confirmation aspects of delivery of the content or enhanced service. The capabilities of block 18b include, but are not limited to: generating centralized VAS codes for mobile operators or third party providers; validating operator/third-party provider VAS codes; mapping operator VAS codes to content; and mapping operator VAS codes to enhanced service provider specific content codes.

[0075] The retailer verification functional block 18c provides the business logic to manage the services that an agent/retailer is able to sell. The capabilities of block 18c include, but are not limited to: determining the availability of value-added services by region and/or by retailer group; and promoting specific value-added services, such as a 'Top 5' or 'Top 10' services, by region and/or by retailer group.

[0076] The VAS pricing and retailer commission block 18d provides the business logic to manage the charges and commissions for the agent/retailer. The capabilities of block 18d include, but are not limited to: managing VAS prices by region(s) and/or retailer distribution

trees, such as by retailer group; and defining and calculating retailer margin by region(s) and/or retailer group(s).

[0077] Lastly, the PIN database block 18e provides the business logic to manage the sets of PINs for the services being offered. The capabilities of this block 18e include, but are not limited to: segmentation of PINs on a per service basis; safe storage of PINs; serving of PINs to the requesting module(s); and the marking of PINs as 'used' once successfully served.

[0078] Communication between the server modules 16, 22, 18, the mobile operator network entities 24, 25, 19 and the third-party service provider network entities 21, 17, 23, are accomplished through interfaces 24a, 25a, 19a, 21a, 17a, 23a, respectively, and a middleware layer 15.

[0079] For each of discussion, the interfaces 24a, 25a, 19a, 21a, 17a and 23a comprise an interface layer, which implements a specific communications protocol. As depicted, each interface is used to separate the connection logic from the business logic, thereby simplifying the integration of mobile operator and third-party network entities. This provides a plug-and-plug environment for standards based network entities.

[0080] In this regard, a primary function of the interface layer is three-fold: (1) to manage the communication sessions with the target platform, such as the color ring tone platform 17; (2) to convert a VAS server 18 request to the required target platform format and send it to the intended target platform; and (3) to interpret the target platform response, and convert that response to an appropriate response for the server modules 16, 22, 18.

[0081] Notably, each interface 24a, 25a, 21a, 17a, 23a and 19a is written for each specific target network entity. For example, the alert interface 23a is written for communication with the information alert platform 23. Similarly, the postpaid interface 19a is written for communication

with the postpaid billing platform 19. Each interface also incorporates features designed to manage the transaction load on a target network entity. This facilitates a seamless plug-and-play integration.

[0082] The middleware layer 15 is configured to standardize and manage the communications between all mobile operator and third-party network entities, and the three server modules 16, 22, 18. It manages core functions and systems, such as: a message-passing system between multiple server modules 16, 22, 18 and the interface layer, preferably using XML; an internal queuing system that routes messages from the server modules 16, 22, 18 and interface layer to internal worker threads; a monitoring system that monitors the status of third-party network connections, internal threads, queues, etc. (with event alarm and logging); initialization and (graceful) shutdown sequences; debug and audit logging; and data collection system that collects performance statistics.

[0083] A more detailed discussion of the transaction management, system monitoring and transaction logging attributes of the middleware layer 15 may be better appreciated with reference to Fig. 3.

[0084] The transaction management attributes of the middleware layer 15 incorporate a range of features to guarantee delivery of transactions so that transactions are never lost. As depicted, messages received from the server modules 16, 18, 22 by the middleware 15 are through dedicated receiver threads 15a. These messages are placed in an inbound queue 15b to await processing. A dedicated worker thread 15c takes the message off queue and processes it. If a response it to be sent, or if the message is to be passed on, then it is placed in an outbound queue 15d. A pooled collection of sending threads 15e then attempt to send the message to its destination server module 18, for instance.

[0085] The system monitoring attributes of the middleware 15 incorporates a range of features that complement transaction management and optimize the performance of the layer. For example, monitoring threads 15f keeps track of all compliance aspects of messages within the server modules 16, 18, 22 and the middleware 15. These compliance aspects include thread activity, message sending and receiving, queue sizes, internal processing statistics, message delivery re-tries, message aging and the like. In addition, a built-in e-mail and SMS alerting system 15g provides notification of important internal events. SMS alerting is possible through Short Message Peer to Peer (SMPP), Simple Network Paging Protocol (SNPP), Universal Computer Protocol (UCP), Computer Interface to Machine Distribution, version 2 (CIMD2) and other protocols. Alerting systems may also include Interactive Voice Response (IVR) systems and Multimedia Messaging System (MMS) with graphical illustrations, if desired. Two other system monitoring attributes include dynamic load balancing (in case of overloading) and dynamic failure recovery (in case of failure).

[0086] The transaction logging attributes of the middleware layer 15 provides a common capability to capture and safe-store data for critical steps in the transaction processing to avoid loss of critical data. Inbuilt even and audit logging to disk 27 provides a continuous trace of message progress. General agent/retailer logging 15h and central transaction logging 15i provides safe storage of critical logs and raw data to a Universal Transaction Logger (UTL) server (not shown).

[0087] The UTL server is a centralized data collection system that captures performance statistics 15j and transaction data in a standardized format so that it is presented in a unified view and extracted by reporting tools. Each transaction is preferably identifiable by service type, transaction type (e.g. balance inquiry, top-up, etc.), date/time, MSISDN, and response code. A

web-based administration graphical user interface (GUI) allows operations and business users to view a range of scenarios, such as viewing an individual service by MSISDN or viewing all services by MSISDN. Preferably, each scenario is controlled by one or more filters.

[0088] In a preferred embodiment, a reporting module communicates with the data collection system to extract data for any individual application, or to consolidate data across all applications. Controlled by one or more filters, the reporting module may create reports for a range of scenarios, such as a report on aggregated services by transaction type (e.g. all top-up transactions by service type). Reports may also be created on aggregated services by retailer/agent or on individual service(s). Through the reporting module, mobile operators or third-party service providers may create their own reports also.

[0089] A more detailed description is now presented regarding operation of the architecture of the present invention to activate delivery of various content and services using a wireless communication device as a transaction gateway.

[0090] Operationally, and with respect to Fig. 4, there is shown a flow chart of a post-paid bill payment transaction using the system of the present invention that enables a mobile phone service subscriber to pay their mobile phone operator's post-paid account using physical currency (i.e., pesos, rupees, pounds, etc.) over the counter to an authorized retailer 10.

[0091] In the exemplary Fig. 4 transaction, the retailer 10 uses a mobile phone 12 as a point-of-sale device to initiate a post-paid bill pay transaction, as at operation 30. In a preferred embodiment, bill pay transactions are performed using a SIM menu by retailers 10 that have authorized electronic wallet permissions and SIM security. The SIM is a subscriber identity module, or a contact-based smart card, that is inserted into a mobile device's handset. The SIM

is configured to store an application on it that is controlled by a menu that is displayed on the mobile device's handset screen, and controlled by the handset's navigation keys.

[0092] Notably, a transaction may be performed using any desired user interface on a variety of mobile based application protocols, such as, but not limited to, short message service (SMS), wireless application protocol (WAP), the Java 2 Platform Micro Edition (J2ME), BREW, etc. Each of the transactions discussed in Figs. 3 through 7 may employ any desired interface/protocol.

[0093] Operation 30 is performed when a mobile phone service subscriber provides the retailer 10 with his/her post-paid mobile phone number, the amount being paid, and a bill reference number. Using the mobile phone device 12, the retailer 10 accesses a M-Commerce server 16 menu.

[0094] Preferably, the SIM application displays the appropriate prompts to the retailer 10 via the SIM menu, such as "Please enter Subscriber Postpaid mobile no."; "Confirm Subscriber Postpaid mobile no."; "Please enter bill reference no."; "Please enter payment amount"; "Enter your M-PIN"; and "Confirm payment of <amount> for Postpaid no. <MSISDN> with ref no. <bill reference no.>". In other words, the retailer 10 selects the corresponding options from the SIM menu, and enters the details provided by the subscriber in operation 30. The retailer 10 then enters its M-Commerce server identification number (i.e. M-PIN) and confirms the transaction.

[0095] The SIM application constructs an encrypted bill pay short message service (SMS) containing the entered data, and sends the message to a SMS center 24, which in turn routes the bill pay message to the M-Commerce server 16. The M-Commerce server 16 determines that the bill pay message is a bill pay transaction, decrypts the message, and authenticates the retailer's 10 details on the e-Wallet server 22, as at operation 32.

[0096] If there are sufficient funds in the retailer's electronic wallet account, the e-wallet server 22 holds the payment amount in reserve and the M-Commerce server 16 initiates a payment request (operation 32) to a billing platform 19 of the mobile operator 10 through the VAS server 18. Preferably, the details of the payment request include information directed to the mobile phone service subscriber's post-paid mobile number (MSISDN), the payment amount, and bill reference number. Optional information may include the payment type and a unique M-Commerce server transaction number.

[0097] At operation 34, the decisional issue is whether a valid post-paid account exists. Here, the billing platform 19 of the mobile operator verifies that the mobile phone service subscriber's MSISDN is a post-paid account by cross-referencing the details of the payment request with information in a post-paid database. If no matching data is found, the billing platform 19 notifies the VAS server 18 of the mismatch, as at operation 36. The VAS server 18 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer 10 and subscriber advising of the failure of the submitted request (operation 38). An example of a subscriber notification SMS message for a failed transaction may read: "<Given name>, there has been a problem processing your bill payment submitted on <submission date> at <submission time>. Please call customer service on <phone number>. Trans # <transaction ID number>."

[0098] On the other hand, if the subscriber is verified as a valid post-paid account, then the billing platform 19 accepts the VAS Server's 18 payment request and posts the payment process, as at operation 40.

[0099] Next, at operation 42, the billing platform 19 sends a confirmation message to the VAS server 18 that payment has been accepted for processing. The VAS server 18 notifies the M-

Commerce server 16, which instructs the e-wallet server 22 to deduct the appropriate payment amount from the retailer's e-wallet account (operation 44).

[00100] The M-Commerce server 16 also constructs a notification SMS message to the mobile phone service subscriber (operation 46) and retailer 10 (operation 48) confirming that payment has been successfully posted. A successful SMS notification message sent to the post-paid mobile phone service subscriber preferably contains information on the customer name, date/time of payment, the retailer's MSISDN, the M-Commerce server's transaction number, and the payment amount. An exemplary form may read: "<Given name>, your bill payment submitted on <submission date> at <submission time> has been successfully processed. Your receipt number is <post-paid receipt #>. Trans # <transaction ID number>."

[00101] Similarly, a successful SMS notification message sent to the retailer 10 preferably contains information on the date/time of the payment, the subscriber's MSISDN, the M-Commerce server's transaction number, and the payment amount. An example retailer notification SMS message for a successfully accepted transaction may read: "On <date> at <time> you submitted <currency amount> for post-paid bill payment of <subscriber MSISDN>. Trans # <transaction ID number>."

[00102] At this juncture, the mobile operator or retailer 10 accepts cash from the mobile phone service subscriber, operation 50.

[00103] It is worth noting that any or all of the VAS content and/or enhanced services, whether digital content or subscription services, is available to pre-paid or post-paid mobile phone subscribers by delivering physical currency over the counter to an authorized retailer 10. Each VAS content or enhanced service is available singly or bundled, and may be enabled or disabled

singly or bundled as desired. Therefore, each VAS content or enhanced service is preferably configured as its own content/service delivery platform on the VAS server 18.

[00104] Referring to Fig. 5 (comprising Figs. 5A and 5B), there is shown an exemplary flow chart of a content purchase transaction in the form of a ring tone purchase transaction using the system of the present invention that enables a pre-pay or post-paid mobile phone subscriber to receive digital content on his/her handset. This is achieved by delivering physical currency to an authorized retailer 10.

[00105] Here, the mobile phone service subscriber selects a specific ring tone, for example, and provides the mobile operator or retailer 10 with the content ID number and his/her mobile phone number. Alternatively and optionally, the subscriber may select a specific logo or picture message. The retailer 10 then uses a mobile phone 12 as a point-of-sale device to initiate the ring tone purchase transaction by accessing a M-Commerce server 16 menu (operation 60).

[00106] Preferably, the SIM application menu displays appropriate prompts for the retailer 10 to enter the data provided by the subscriber. The SIM menu may include such prompts as: "Please enter Purchasing Subscriber mobile number"; "Please enter Target Subscriber mobile number" (if this entry is left blank, then the system defaults to the subscriber's MSISDN); "Please enter Content ID"; "Enter your M-PIN"; "Confirm sale of <Content ID> to "MSISDN>". After the retailer 10 enters its merchant identification number (i.e. M-PIN), the retailer 10 confirms the transaction.

[00107] Note the option to include a different 'target' MSISDN in addition to the subscriber's MSISDN, if desired. This option allows the mobile phone service subscriber to purchase VAS content or enhanced service(s) for family members, friends, colleagues, and others.

[00108] The SIM application constructs an encrypted content purchase SMS message containing the entered data, and sends the message to a SMS center 24, which in turn routes the content purchase message to the M-Commerce server 16. The M-Commerce server 16 then determines that the content purchase SMS message is a content purchase transaction, decrypts the message, and authenticates the retailer's details on the e-Wallet server 22 (operation 61). In addition, the M-Commerce server 16 forwards a delivery request to the VAS server 18, passing along the retailer's MSISDN and the content ID.

[00109] At operation 62, a decisional issue is whether the retailer 10 is authorized to sell the designated content. The goal here is to prevent the unauthorized sale of electronic content by an unauthorized retailer 10 in addition to preventing the sale of unauthorized content to a mobile phone service subscriber. If the retailer 10 is not authorized to sell the designated content, the VAS server 18 does not validate the retailer 10 for that sale transaction. Accordingly, the VAS server 18 sends a non-validation notification to the M-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber that the transaction was unsuccessful (operation 63).

[00110] On the other hand, if the retailer 10 is determined to be authorized to sell the designated content, the next decisional issue is whether the mobile operator's content ID is valid (operation 64). If not, the VAS server 18 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer 10 and the mobile phone service subscriber advising of the failure of the submitted request (operation 63). Exemplary failure notification SMS messages are as earlier described.

[00111] However, if the operator's content ID is valid, then the VAS server 18 retrieves the corresponding mobile operator's (or other authorized content provider's) content ID, retail price

and retailer commission and passes this information to the M-Commerce server 16. The M-Commerce server 16 requests the e-Wallet server 22 to verify that the retailer has sufficient funds in its wallet and to reserve the retail price less retailer commission. The M-Commerce server 16 then requests the VAS server 18 to initiate the content delivery request to the vendor content delivery platform 21 (operation 65), preferably passing along the target mobile phone service subscriber's MSISDN, content ID and M-Commerce server transaction ID.

[00112] The next question now is whether the vendor content ID is valid (operation 66). If not, the vendor content delivery platform 21 sends a non-validation notification that the vendor ID is invalid to the VAS server 18. The VAS server 18 notifies the M-Commerce server 16, which then sends a notification SMS message to the retailer 10, the vendor, and the mobile phone service subscriber advising of the failure of the submitted request (operation 67).

[00113] On the other hand, if the vendor content ID is deemed valid, the vendor content delivery platform 21 sends the designated content to the SMS center 24 (operation 68).

[00114] At operation 70, the SMS center 24 sends the content (i.e. the selected ring tone) to the mobile phone service subscriber's handset as a once-only, one-shot dispatch. In other words, there are no transmission re-tries of the content. The SMS center 24 then receives the delivery receipt and returns delivery confirmation to the vendor content delivery platform 21 (operation 72), which confirms the content delivery was successful (operation 74) and sends a positive response back to the VAS server 18.

[00115] The VAS server 18 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the payment amount from the retailer's electronic wallet account (operation 76). Accordingly, the M-Commerce server 16 sends a notification SMS message to the mobile

phone service subscriber (operation 78) and retailer 10 (operation 80) confirming that the content has been successfully delivered.

[00116] The respective notification messages are as similar to the ones earlier described. For example, where the subscriber has provided target subscriber information, then a successfully SMS notification message may contain the following information: date/time, the retailer's MSISDN, the target subscriber's MSISDN, the e-wallet platform's transaction number, and the payment amount.

[00117] The retailer 10 collects the currency from the subscriber (operation 82) to end the transaction.

[00118] In instances where a transaction is unsuccessful, the reserved amount from the retailer's e-wallet is cancelled and the e-wallet is not debited.

[00119] Referring now to Fig. 6 (comprising Figs. 6A and 6B), a flow chart of an enhanced service subscription purchase transaction in the form of a color ring tone, is illustrated. A color ring tone (or 'ring back tone') is best described as an audio file, which is usually a recording of a song, that a caller hears when the caller calls another subscriber of the color ring tone service. The song replaces the normal telephone ring tone that one would otherwise hear when one calls another. The audio file is preferably, though not necessarily, stored on a central server connected to a mobile operator's network.

[00120] In the transaction depicted in Fig. 6, the pre-pay or post-paid mobile phone service subscriber provides the retailer 10 with his/her mobile phone number (MSISDN) to subscribe to the color ring tone service. The retailer 10 then uses a mobile phone 12 as a point-of-sale device to initiate the color ring tone subscription transaction from the SIM menu (operation 90).

[00121] Preferably, the SIM application menu displays appropriate prompts, as earlier described, for the retailer 10 to enter the data provided by the subscriber. The retailer 10 then enters its M-PIN and confirms the transaction. Alternatively and/or optionally, the SIM menu may provide for the entering of a target subscriber MSISDN, which is different from the subscriber's MSISDN. This enables subscribers to purchase gift VAS service(s) for family, friends and others.

[00122] The SIM application constructs an encrypted color ring tone subscription SMS message containing the entered data, and sends the message to a SMS center 24. The SMS center 24 routes the color ring tone subscription message to the M-Commerce server 16, which determines that the color ring tone subscription message is a color ring tone subscription transaction, decrypts the message, and authenticates the retailer's details (operation 91) on the e-Wallet server 22. In addition, the M-Commerce server 16 forwards a subscription request to the VAS server 18 (operation 91), preferably passing along the retailer's MSISDN and the content ID.

[00123] At operation 92, a decisional issue is whether the retailer 10 is authorized to sell the designated enhanced service. The goal here is to prevent the unauthorized sale of subscription services by an unauthorized retailer 10 in addition to preventing the sale of unauthorized enhanced services to a mobile phone service subscriber. If the retailer 10 is not authorized to sell the designated enhanced service, the VAS server 18 does not validate the retailer 10 for that sale transaction. The VAS server 18 sends a non-validation notification to the M-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber that the transaction was unsuccessful (operation 93).

[00124] If the retailer 10 is deemed to be authorized to sell the designated enhanced service, the next question is whether the mobile operator's content ID is valid (operator 94). If not, the VAS

server 18 does not validate the mobile operator for that sale transaction. The VAS server 18 sends a non-validation notification to the M-Commerce server 16, which then sends a notification SMS message to the retailer 10, the mobile operator and the mobile phone service subscriber that the transaction was unsuccessful (operation 93).

[00125] However, if the operator content ID is deemed valid, then the VAS server 18 retrieves the corresponding mobile operator's (or other authorized content provider's) content ID, retail price and retailer commission and passes this information to the M-Commerce server 16. The M-Commerce server 16 requests the e-Wallet server 22 to verify that the retailer has sufficient funds in its electronic wallet and to reserve the retail price less retailer commission. The M-Commerce server 16 then requests the VAS server 18 to initiate the subscription request to the color ring tone platform 17 (operation 95), preferably passing along the target mobile phone service subscriber's MSISDN, content ID and M-Commerce server transaction ID.

[00126] The next decisional issue is whether the subscriber has already subscribed to the color ring tone subscription service (operation 96). If so, the color ring tone platform 17 sends a notification to the VAS server 18 that the subscriber is already subscribed (operation 98). The VAS server 18 notifies the M-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber advising that the subscriber is already an existing customer (operation 99).

[00127] However, if the subscriber has not previously subscribed to the color ring tone service, then the color ring tone platform 17 activates a subscription for the desired subscriber MSISDN (operation 100). The color ring tone platform 17 then sends confirmation to the VAS server 18 that the subscription process has been initiated (operation 102). The VAS server 18 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the payment amount,

preferably a recommended retail price less commission, from the retailer's electronic wallet account (operation 104), and sends a notification SMS message to the subscriber (operation 106) and retailer 10 (operation 108) confirming that the subscription request has been registered and when service will be provided. The respective notification messages are similar to the ones earlier described.

[00128] The retailer 10 collects the currency from the subscriber (operation 110). When the color ring tone platform 17 completes the subscription process, it sends a notice to the subscriber confirming successful provisioning of the service (operation 112).

[00129] The decisional operations of Fig. 7 (comprising Figs. 7A and 7B) showing a flow chart of an enhanced service subscription purchase transaction in the form of a color ring tone song purchase, in accordance with the present invention, is similar to the decisional operations of Fig. 6, except that the transaction is allowed to proceed only if the subscriber has previously subscribed to the service. In other words, if the mobile phone user was not previously subscribed, then the subscriber and retailer receive notifications instructing the user to subscribe to the color ring tone service first.

[00130] To explain further, referring to Fig. 7A, the subscriber provides the retailer 10 with his/her selection of a desired song by way of a content ID number and his/her mobile phone number. The retailer 10 then uses a mobile phone 12 as a point-of-sale device to initiate the song purchase transaction (operation 120).

[00131] Preferably, the SIM application menu displays appropriate prompts for the retailer 10 to enter the data provided by the subscriber. For example, the SIM menu may include such prompts as: "Please enter Purchasing subscriber mobile number"; "Please enter Target Subscriber mobile number"; "Please enter Content ID"; "Enter your M-PIN"; "Confirm sale of

<content ID> to <MSISDN>". The retailer 10 enters its merchant identification number (i.e. M-PIN) and confirms the transaction.

[00132] Note the option to include a prompt directed to target subscriber information, if desired. This option allows the mobile phone service subscriber to purchase VAS content and/or enhanced services for one or more family members, friends and others as a gift.

[00133] The SIM application preferably constructs an encrypted song selection SMS message containing the entered data, and sends the message to a SMS center 24, which in turn routes the song purchase SMS message to the M-Commerce server 16, which determines that the song purchase SMS message is a song purchase transaction, decrypts the message, and authenticates the retailer's details (operation 121) on the e-Wallet server 22. Additionally, the M-Commerce server 16 transmits an initiate-song request to the VAS server 18, passing along the retailer's MSISDN and the content ID.

[00134] At operation 122, a decisional issue is whether the retailer 10 is authorized to sell the designated enhanced service. The goal here is to prevent the unauthorized sale of subscription services by an unauthorized retailer 10 in addition to preventing the sale of unauthorized enhanced services to a mobile phone service subscriber. If the retailer 10 is not authorized to sell the designated enhanced service, the VAS server 18 does not validate the retailer 10 for that sale transaction. The VAS server 18 sends a non-validation notification to the m-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber that the transaction was unsuccessful (operation 123).

[00135] If the retailer 10 is deemed to be authorized to sell the designated enhanced service, the next question is whether the mobile operator's content ID is valid (operation 124). If not, the VAS server 18 does not validate the mobile operator for that sale transaction. The VAS server

18 sends a non-validation notification to the m-Commerce server 16, which then sends a notification SMS message to the retailer, the mobile operator and the mobile phone service subscriber that the transaction was unsuccessful (operation 123).

[00136] However, if the operator content ID is deemed valid, then the VAS server 18 retrieves the corresponding mobile operator's (or other authorized content provider's) content ID, retail price and retailer commission and passes this information to the M-Commerce server 16. The M-Commerce server 16 requests the e-Wallet server 22 to verify that the retailer has sufficient funds in its electronic wallet and to reserve the retail price less retailer commission. The M-Commerce server 16 then requests the VAS server 18 to initiate the song request to the color ring tone platform 17 (operation 125), preferably passing along the target mobile phone service subscriber's MSISDN, content ID and M-Commerce server transaction ID.

[00137] The next decisional issue is whether the subscriber is already a subscribing customer (operation 126). If not, the color ring tone platform 17 sends a response to the VAS server 18 that the subscriber is not a current customer (operation 128). The VAS server 18 notifies the M-Commerce server 16, which then sends a notification SMS message to the subscriber and retailer 10 advising the subscriber of the need to enroll in the subscription first (operation 129). The failure notification message is similar to earlier ones described herein.

[00138] However, if the subscriber is found to be an existing customer, then the color ring tone platform 17 activates the selected song request and delivers the selected song to the subscriber (operation 130). The color ring tone platform 17 also sends confirmation to the VAS server 18 that the song has been delivered (operation 132). The VAS server 18 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the payment amount, preferably a recommended retail price less commission, from the retailer's electronic wallet account

(operation 134), and sends notification messages to the subscriber (operation 136) and retailer 10 (operation 138) confirming that the selected song was activated for the pre-pay or postpaid mobile phone subscriber's service. The respective notification messages are similar to the ones earlier described. At operation 140, the retailer 10 collects cash currency from the subscriber.

[00139] Referring now to Fig. 8 (comprising Figs. 8A and 8B), there is shown a flow chart of an enhanced service purchase transaction in the form of a virtual calling card. In this instance, the subscriber generally requests a card product, such as a virtual calling card or a VAS card, from the retailer 10. Using the mobile phone 12 as a point-of-sale device, the retailer 10 initiates a card purchase transaction from the SIM menu (operation 150), entering pertinent details provided by the subscriber.

[00140] As earlier described, the SIM menu is user-friendly, providing appropriate prompts of the necessary input information. In addition, the menu similarly provides for the option of gift card or VAS service(s) purchase for family and friends.

[00141] Upon confirmation of the transaction by the retailer 10, the SIM application constructs an encrypted virtual calling card and/or VAS card SMS message containing the entered data, and sends the message to a SMS center 24. For simplicity, the discussion will be had to a calling card product although it may be a calling card and/or a VAS card.

[00142] The SMS center 24 routes the card purchase SMS message to the M-Commerce server 16, which determines that the card purchase SMS message is a calling card purchase transaction, decrypts the message, and authenticates the retailer 10 details (operation 151) on the e-Wallet server 22. Additionally, the M-Commerce server 16 transmits a retrieve PIN request to the VAS server 18, passing along the Retailer's MSISDN and the service ID.

[00143] At operation 152, a decisional issue is whether the retailer 10 is authorized to sell the designated enhanced service. The goal here is to prevent the unauthorized sale of calling card services by an unauthorized retailer 10 in addition to preventing the sale of unauthorized enhanced services to a mobile phone service subscriber. If the retailer 10 is not authorized to sell the designated enhanced service, the VAS server 18 does not validate the retailer 10 for that sale transaction. The VAS server 18 sends a non-validation notification to the M-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber that the transaction was unsuccessful (operation 153).

[00144] If the retailer 10 is deemed to be authorized to sell the designated enhanced service, the next question is whether the mobile operator's content ID is valid (operation 154). If not, the VAS server does not validate the mobile operator for that sale transaction. The VAS server 18 sends a non-validation notification to the m-Commerce server 16, which then sends a notification SMS message to the retailer 10, the mobile operator and the mobile phone service subscriber that the transaction was unsuccessful (operation (153)).

[00145] However, if the operator content ID is deemed valid, then the VAS server 18 retrieves the corresponding mobile operator's (or other authorized content provider's) content ID, retail price and retailer commission and passes this information to the M-Commerce server 16. The M-Commerce server 16 requests the e-Wallet server 22 to verify that the retailer has sufficient funds in its electronic wallet and to reserve the retail price less retailer commission. The M-Commerce server 16 then requests the VAS server 18 to initiate a calling card PIN request to the vendor content delivery platform 21 (operation 155), preferably passing along the target mobile phone service subscriber's MSISDN, content ID and M-Commerce server transaction ID. The vendor content delivery platform returns a content ID validation notification to the VAS server

18, which selects an identification number (PIN) from a calling card PIN database (operation 156).

[00146] At operation 158, the VAS server 18 transmits a SMS message containing the PIN to the SMS center 24, which in turn dispatches a message to the target MSISDN as a once-only transmission (operation 159). The SMS center 24 receives a receipt of the calling card information delivery and passes along the delivery receipt confirmation to the VAS server 18 (operation 160), which confirms the content delivery was successful (operation 161) and sends a positive response back to the M-Commerce server 16.

[00147] The M-Commerce server 16 instructs the e-Wallet server 22 to deduct the payment amount, preferably the recommended retail price less retailer commission, from the retailer's electronic wallet account (operation 162). The M-Commerce server 16 sends a notification SMS message to the subscriber (operation 164) and retailer 10 (operation 166) confirming that the PIN was successfully delivered. The respective notification messages are similar to the ones earlier described. The transaction concludes when the retailer 10 collects cash currency from the mobile phone service subscriber (operation 168).

[00148] Referring now to Fig. 9 (comprising Figs. 9A and 9B), a flow chart of an enhanced service subscription purchase transaction in the form of an alert service, using the system of the present invention, is illustrated. In this scenario, the subscriber provides the retailer 10 with his/her selection of information alert(s), such as news, weather, or the like, and mobile phone number (MSISDN) to subscribe to the information alert service. The retailer then uses a mobile phone 12 as a point-of-sale device to initiate the information subscription purchase transaction from the SIM menu (operation 170).

[00149] Preferably, the SIM application menu displays appropriate prompts, as earlier described, for the retailer 10 to enter the data provided by the subscriber. The retailer 10 then enters its M-PIN and confirms the transaction. Alternatively and/or optionally, the SIM menu may provide for the entering of a target subscriber MSISDN, which is different from the subscriber's. This enables subscribers to purchase one or more gift VAS services for family, friends and others.

[00150] The SIM application constructs an encrypted information alert subscription SMS message containing the entered data, and sends the message to a SMS center 24. The SMS center 24 routes the information alert subscription message to the M-Commerce server 16, which determines that the information alert subscription SMS message is an information alert subscription transaction, decrypts the message, authenticates the retailer's details on the e-Wallet server 22 (operation 171).

[00151] At operation 172, a decisional issue is whether the retailer 10 is authorized to sell the designated enhanced service. The goal here is to prevent the unauthorized sale of subscription services by an unauthorized retailer 10 in addition to preventing the sale of unauthorized enhanced services to a mobile phone service subscriber. If the retailer 10 is not authorized to sell the designated enhanced service, the VAS server 18 does not validate the retailer 10 for that sale transaction. The VAS server 18 sends a non-validation notification to the M-Commerce server 16, which then sends a notification SMS message to the retailer 10 and mobile phone service subscriber that the transaction was unsuccessful (operation 173).

[00152] If the retailer 10 is deemed to be authorized to sell the designated enhanced service, the next question is whether the mobile operator's content ID is valid (operation 174). If not, the VAS server 18 does not validate the mobile operator for that sale transaction. The VAS server

18 sends a non-validation notification to the m-Commerce server 16, which then sends a notification SMS message to the retailer 10, the mobile operator and the mobile phone service subscriber that the transaction was unsuccessful (operation 93).

[00153] However, if the operator content ID is deemed valid, then the VAS server 18 retrieves the corresponding mobile operator's (or other authorized content provider's) content ID, retail price and retailer commission and passes this information to the M-Commerce server 16. The M-Commerce server 16 requests the e-Wallet server 22 to verify that the retailer has sufficient funds in their wallet and to reserve the retail price less retailer commission. The M-Commerce server 16 then requests the VAS server 18 to initiate the subscription request to the information alert platform 23 (operation 175), preferably passing along the target mobile phone service subscriber's MSISDN, content ID and M-Commerce server transaction ID.

[00154] At operation 176, the next decisional issue is whether the subscriber is already a customer of the information alert subscription service. If so, the information alert platform 23 informs the VAS server 18 that the subscriber is already subscribed (operation 178). The VAS server 18 notifies the M-Commerce server 16, which then sends a notification SMS message to inform the mobile phone service subscriber and retailer 10 that the subscriber is already an existing customer (operation 179).

[00155] However, if the subscriber is not an existing customer of the subscription service, then the information alert platform 23 activates a subscription for the specified alert service (operation 180). The information alert platform 23 then sends a confirmation to the VAS server 18 that the subscription process has been initiated and was successful (operation 182). The VAS server 18 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the payment amount, preferably the recommended retail price less commission, from the retailer's

electronic wallet account (operation 184), and sends a notification SMS message to the subscriber (operation 186) and the retailer 10 (operation 188) confirming successful subscription. The respective notification messages are similar to the ones earlier described. The transaction concludes when the retailer 10 collects cash currency from the subscriber (operation 190).

[00156] In Fig. 10, there is shown yet another exemplary embodiment of a system for enabling a wireless communication device as a point-of-sale (POS) device. As depicted, the wireless communication device 12, such as a mobile phone, is used by a retailer or mobile operator 10 as a POS device to access the M-Commerce server 16 through GSM 14.

[00157] Through communication with M-Commerce server 16, the wireless device 12 provides another menu of options of electronic or digital products. These products may be supplied by one or more third party providers in the form of third party provider platforms 200, 300, 400, 500, etc., which systems operate in tandem with a mobile operator's system(s).

[00158] In this embodiment, the M-Commerce server 16 also provides operational logic to manage an end-to-end M-Commerce transaction between the wireless device 12 and the third party provider platforms 200, 300, 400 and 500 depicted. The operational logic includes, but is not limited to: an interface logic – such as wireless application protocol (WAP), short message service (SMS), Java 2 Platform Micro Edition (J2ME), SIM Application Toolkit (STK), etc. – for integration with a retailer's or mobile operator's access channels; parsing logic to receive and process transactions from various access devices using the above-mentioned interface logic; a transaction management logic to control performance of desired transactions such as third party provider bill payment transactions and the like; integration capabilities to facilitate integration with one or more sub-systems, such as the e-wallet server 22, and each of the third party provider platforms 200, 300, 400, 500, etc.; and other operational support capabilities including but not

limited to system configuration, mapping and validation of retailer or wireless operator content ID, authenticating authority for retailers to provide specified bill pay services, establishing retail prices and commissions, reporting, auditing, etc.

[00159] The third party provider platform 200 may represent a utility company that provides electricity to customers. Platform 200, which preferably exists in the network of Electric Company A, is hardware and software used to house or store the files necessary to effect payment of Company A's electric bill by a customer or customer's agent. In the provisioning of bill payment services for Electric Company A, platform 200 is interconnected to the switching infrastructure of retailer or wireless operator 10 via device 12 to electronically post payment to a customer's electric account with Electric Company A thus allowing the retailer 10 to collect currency payment from the customer.

[00160] The third party provider platform 300 may represent another utility company such as one that provides gas to customers. Platform 300, which preferably exists in the network of Gas Company B, is hardware and software used to house or store the files necessary to effect payment of Company B's gas bill by a customer / customer's agent. In the provisioning of bill payment services for Gas Company B, platform 300 is interconnected to the switching infrastructure of retailer or wireless operator 10 via device 12 to electronically post payment to a customer's gas account with Gas Company B thus allowing the retailer 10 to collect currency payment from the customer.

[00161] The third party provider platform 400 may represent any one of the many credit card companies (i.e. American Express, Visa, MasterCard, etc.) and/or issuing financial services companies (Citibank, Bank of America, Credit Suisse, etc.). Platform C, which preferably exists in the network of each credit card and/or financial services company, is hardware and software

used to house or store the files necessary to effect payment of Company C's credit card bill by a customer / customer's agent. In the provisioning of bill payment services for credit card Company C, platform 400 is interconnected to the switching infrastructure of retailer 10 via device 12 to electronically post payment to a customer's credit card account with Company C thus allowing the retailer 10 to collect currency payment from the customer.

[00162] In yet another example, the third party provider platform 500 may represent another utility company such as one that provides water to customers. Platform 500, which preferably exists in the network of Water Company ABC, is hardware and software used to house or store the files necessary to effect payment of Company ABC's water bill by a customer / customer's agent. In the provisioning of bill payment services for Water Company ABC, platform 500 is interconnected to the switching infrastructure of retailer or wireless operator 10 via device 12 to electronically post payment to a customer's water account with Water Company ABC thus allowing the retailer 10 to collect currency payment from the customer.

[00163] A more detailed illustration of a preferred embodiment of the application architecture of the embodiment of Fig. 10 is shown in Fig. 11. The application architecture performs all of the transaction processing functions, and manages integration amongst and between the server modules 16, 18, 20, 22, 600, its sub-systems, the middleware 15, the various platforms 200, 300, 400, 500, 17, 19, 21, 23, the gateway(s) 25, server(s) 26, as well as any mobile operator / third party / vendor network entities, such as the SMS center 24. The application architecture also manages the back-end administration, reporting and monitoring infrastructure.

[00164] As depicted in Fig. 10, the M-Commerce server 16, e-Wallet server 22 and a third party billing server 600 may be viewed as the primary modules developed to support any number of third party bill payment applications. This is the application layer. These modules contain the

business logic for each particular solution, and are separated into discrete functional blocks, which interact with each other and with the middleware and interface layers. In another aspect of this embodiment, the system for the third party billing server 600 may be integrated within each of the third party billing companies 200, 300, 400, 500.

[00165] From the exemplary embodiments provided above, each platform 200, 300, 400, 500, etc., corresponds to a separate and different third party provider. Notably, third party platforms may be used to sell and/or collect payments for a wide variety of goods and services. The following list is but a small subset of the full range of sales and/or payments that may be employed using the technology of the present invention. These include, but are not limited to, bill payment systems to pay for: satellite radio subscriptions, satellite television, internet service provider (ISP) services, ticket purchases (whether for travel, promotional events, sporting events, the lottery, etc.), donations, utilities (i.e. electric bills, water bills, gas bills, etc.), local/state/national tax debts, financial services, insurance premiums, mortgages, credit card monthly installment, education tuition fees, etc. Application of the present invention includes bill payment systems to pay for web-based / e-commerce services, which includes a wide variety of electronic products and services (e.g. online accounts for eBay, Amazon, music portals, gaming, library subscriptions, internet telephony, internet messenger services, television shopping, etc.). This invention is not limited to bill payment (collection) systems only. It is operational for disbursement systems as well where a customer receives currency from the retailer 10.

[00166] The description of the M-Commerce server 16 is as earlier described.

[00167] Similarly, the description of the e-Wallet server 22 is as earlier described with appropriate modifications for the routing of transactions from/to the M-Commerce server 16 and the third party billing server 600 associated with each of the third party platforms 200, 300, 400,

500, etc., to effect the necessary bill payment transaction(s). Additionally and/or optionally, another e-Wallet server, representing a customer's electronic wallet (not shown), may be included in the exemplary embodiment of Fig. 10 to manage interactions with the customer's virtual account.

[00168] The last of the three primary modules depicted in the exemplary embodiment of Fig. 10 is the third party billing server 600, which comprises five main functional blocks; namely, a third party transaction management block 600a, a retailer verification block 600c, a third party retailer commission block 600d, and a PIN database block 600e.

[00169] The third party billing server transaction management block 600a provides the business logic to manage the transaction aspects of delivery of billing payment content or services. The capabilities of block 600a include, but are not limited to: routing transactions from/to the M-Commerce, e-Wallet and third party billing servers 16, 22, 600, respectively, (and optionally a customer e-Wallet (not shown)); routing transactions from/to the interfaces 200a, 300a, 400a, 500a for the platforms 200, 300, 400, 500, respectively; and transaction data logging for third party billing auditing and reporting.

[00170] The retailer verification functional block 600c provides the business logic to manage the services that a third party provider is able to provide. The capabilities of block 600c include, but are not limited to: determining the availability of bill payment services by vendor, by region or third party provider group.

[00171] The third party provider retailer commission block 600d provides the business logic to manage the charges and commissions for the retailer/third party provider/agent. The capabilities of block 600d include, but are not limited to: managing prices by region(s) and/or retailer/third party provider distribution trees, such as by retailer/third party provider group; and defining and

calculating retailer/third party provider margin by region(s) and/or retailer/third party provider group(s).

[00172] Lastly, the PIN database block 600e provides the business logic to manage the sets of PINs for the bill payment services being offered. The capabilities of block 600e include, but are not limited to: segmentation of PINs on a per service basis; safe storage of PINs; serving of PINs to the requesting module(s); and the marking of PINs as “used” once successfully served.

[00173] Communication between the server modules 16, 22, 600 and the one or more operator/third party service provider network entities, such as the SMS center 24, the WAP gateway 25, and the platforms 200, 300, 400, 500, 21, 17, 23, 19, is accomplished through interfaces 200a, 300a, 400a, 500a, 24a, 25a and a middleware layer 15.

[00174] For each of discussion, the interfaces 200a, 300a, 400a, 500a, 24a and 25a comprise an interface layer, which implements a specific communications protocol. As depicted, each interface is used to separate the connection logic from the business logic, thereby simplifying the integration of third party network entities. This provides a plug-and-plug environment for standards based network entities.

[00175] In this regard, a primary function of the interface layer is three-fold: (1) to manage the communication sessions with the target third party platform, such as Water Company ABC platform 500; (2) to convert a third party billing server 600 request to the required target platform format and send it to the intended target platform; and (3) to interpret the target platform response, and convert that response to an appropriate response for the server modules 16, 22, 600.

[00176] Notably, each interface 200a, 300a, 400a, 500a, 24a, 25a is written for each specific target third party bill pay service provider entity. For example, the credit card company interface

400a is written for communication with credit card Company C bill pay platform 400. Similarly, the gas company interface 300a is written for communication with the Gas Company B platform 300. Each interface also incorporates features designed to manage the transaction load on a target third party service provider entity. This facilitates a seamless plug-and-play integration.

[00177] A more detailed description is now presented regarding operation of the architecture of the embodiment of Figs. 10 and 11 to activate bill payment services using a wireless communication device.

[00178] Operationally, and with respect to Fig. 12, there is shown a flow chart of a third party bill payment transaction using the system of the embodiment of Figs. 10 and 11 that enables a customer of Water Company ABC to pay his/her water bill using physical currency (i.e. pesos, rupees, pounds, etc.) over the counter to an authorized retailer 10 via device 12.

[00179] In the exemplary Fig. 12 transaction, a customer engages the retailer 10 to pay the customer's water bill with Water Company ABC via Water Company ABC platform 500. Importantly, only third party service providers, which platforms are integrated into M-Commerce server 16 may provide bill payment transactions using the technology of the present invention.

[00180] Once a customer engages a retailer 10 to pay his/her water bill, the retailer 10 uses a wireless device 12 as a point-of-sale device to initiate a third party bill pay transaction, as at operation 510. In a preferred embodiment, bill pay transactions are performed using a SIM menu by retailers 10 that have authorized electronic wallet permissions and SIM security. Characteristics of SIM are as earlier described. In addition, the different options that may be provided in the SIM menu include, for example: (a) Prepaid Topup; (b) Postpaid Bill Pay; (c) VAS Selling; (d) Water Company ABC Bill Pay; (e) Water Company XYZ Bill Pay; (f) Credit

Card Bill Pay; (g) Gas Company DEF Bill Pay; (h) Electric Company A Bill Pay; (i) GHI Electronic PINS; (j) HIJ Cash Withdrawal; etc.

[00181] In keeping with the customer's stated desire to pay his/her water bill from Water Company ABC, retailer 10 selects option "(d) Water Company ABC Bill Pay". This menu requires retailer 10 to provide three pieces of information; namely, (i) the customer's (unique) identifier by which the customer is recognized by the third party billing entity, which in this case is Water Company ABC. This identifier may generally comprise the customer's account number in the Water Company's billing system; (ii) the desired payment amount; and (iii) the retailer's M-Commerce server identification number (i.e. M-PIN).

[00182] Preferably, the SIM application displays the appropriate prompts to the retailer 10 via the SIM menu. In other words, the retailer selects the corresponding option (i.e. option (d)) from the SIM menu, and enters the two pieces of information provided by the customer in operation 30, then enters its M-PIN and confirms the transaction.

[00183] The SIM application constructs an encrypted bill pay short message service (SMS) containing the entered data, and sends the message to a SMS center 24, which in turn routes the bill pay message to the M-Commerce server 16. The M-Commerce server 16 determines that the bill pay message is a bill pay transaction, decrypts the message, and authenticates the retailer's 10 details on the e-Wallet server 22, as at operation 512.

[00184] If there are sufficient funds in the retailer's electronic wallet account, the e-Wallet server 22 holds the payment amount in reserve and the M-Commerce server 16 initiates a payment request (operation 514) to a billing platform 500 of Water Company ABC through the third party billing server 600. Preferably, the details of the payment request include three pieces of information provided by the customer; namely, (i) the customer's (unique) identifier by which

the customer is recognized by the third party billing entity, which in this case is Water Company ABC; (ii) the desired payment amount; and (iii) the customer's wireless device number (i.e. MSISDN). Optional information may include the payment type and a unique M-Commerce server transaction number.

[00185] At operation 516, the decisional issue is whether a valid customer water account exists. Here, the billing platform 500 of Water Company ABC verifies that the customer's water bill account is a valid one by cross-referencing of the payment request with information in a water account database. If no matching data is found, Water Company ABC's billing platform 500 notifies the third party billing server 600 of the mismatch, as at operation 518. The third party billing server 600 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer 10 via device 12, advising of the failure of the submitted request (operation 520). Alternatively, if the customer's MSISDN identifier was earlier provided, the M-Commerce server 16 also sends a notification SMS message to the customer (via a wireless device), informing that the submitted request failed.

[00186] On the other hand, if the customer's water bill account is verified as a valid account, then Water Company ABC's billing platform 500 accepts the third party billing server's 600 payment request and posts the payment process, as at operation 522.

[00187] Next, at operation 524, the Water Company ABC platform 500 sends a confirmation message to the third party billing server 500 that payment has been accepted for processing. The third party billing server 600 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the appropriate payment amount from the retailer's e-Wallet account (operation 526).

[00188] The M-Commerce server 16 also constructs a notification SMS message to the customer's wireless device, if any, (operation 528) and retailer 10 (operation 530) confirming that payment has been successfully posted. A successful SMS notification message sent to the customer's wireless device preferably contains information on the customer's name, date/time of payment, the retailer's name, the M-Commerce server's transaction number, and the payment amount.

[00189] Similarly, a successful SMS notification message sent to the retailer 10 preferably contains information on the date/time of payment, the customer's MSISDN, the M-Commerce server's transaction number, and the payment amount.

[00190] At this juncture, the retailer 10 accepts currency from the customer in the payment amount (operation 532).

[00191] Referring now to Fig. 13, there is shown another flow chart of a third party bill payment transaction using the system of the embodiment of Figs. 10 and 11 that enables a customer to purchase online time.

[00192] In the exemplary Fig. 13 transaction, a customer engages the retailer 10 to pay for an electronic PIN that allows the customer a specified amount of online time for a desired purpose, such as 30 minutes of online gaming playing time. Generally, an electronic PIN refers to any unique alphanumeric code usually generated using an algorithm. Here, the retailer 10 selects option "(i) GHI Electronic PINS" from the SIM Menu displayed on the wireless device 12, in effect initiating a third party bill pay transaction, as at operation 522. Upon selecting option (i), another menu requires the retailer 10 to provide three pieces of information – (a) the customer's (unique) identifier such as the customer's mobile number; (b) the desired category PIN, which may have one or more varying payment amounts or time; and (c) the retailer's M-Commerce

server identification number (i.e. M-PIN), to verify authorized use. Once the information is inputted, the application seeks accuracy confirmation of the information / transaction.

[00193] The SIM application constructs an encrypted bill pay short message service (SMS) containing the entered data, and sends the message to a SMS center 24 (via GSM network 14), which in turn routes the bill pay message to the M-Commerce server 16. The M-Commerce server 16 determines that the bill pay message is a bill pay transaction, decrypts the message, and authenticates the retailer's 10 details on the e-Wallet server 22, as at operation 524.

[00194] If there are sufficient funds in the retailer's electronic wallet account, the e-Wallet server 22 holds the payment amount in reserve and the M-Commerce server 16 initiates a payment request (operation 526) to the third party billing server 600. Preferably, the details of the payment request additionally include the retailer's MSISDN and details of menu option (i), usable to identify that the electronic PIN request option was previously selected.

[00195] The third party retailer verification block 600c also verifies that the retailer is an authorized one (operation 530). If no matching data is found, the billing server 600 notifies the M-Commerce server 16 of the mismatch (operation 532). The M-Commerce server 16 in turn sends a notification SMS message to the retailer 10 advising of the failure of the submitted request (operation 534).

[00196] Once authorized, the third party retailer verification block 600c communicates verification to the transaction management block 600a, which accepts and posts the payment processing (operation 536). Accordingly, at operation 538, the third party billing server 600 notifies the M-Commerce server 16, which instructs the e-Wallet server 22 to deduct the appropriate payment amount from the retailer's e-Wallet account (operation 538), and which retrieves an electronic PIN stored in PIN database 600e (operation 540).

[00197] The M-Commerce server 16 also constructs a notification SMS message to the customer's wireless device (operation 542) and retailer 10 (operation 544) confirming that payment has been successfully posted and delivering the electronic PIN to the customer only. A successful SMS notification message sent to the customer's wireless device preferably also contains information on the customer's name, date/time of payment, the retailer's name, the M-Commerce server's transaction number, and the payment amount. Similarly, a successful SMS notification message sent to the retailer 10 preferably also contains information on the date/time of payment, the customer's MSISDN, the M-Commerce server's transaction number, and the payment amount.

[00198] At this juncture, the retailer or wireless operation 10 accepts currency from the customer (operation 546). Once the customer receives the electronic PIN, the customer may now log onto GHI's website and enter the above-received electronic PIN, which allows the customer 30 minutes of online gaming playing time.

[00199] Referring now to Fig. 14, there is shown another flow chart illustrating a third party disbursement transaction using the system of the embodiment of Figs. 10 and 11 that enables a customer to withdraw currency from his/her financial account. In this exemplary scenario, a financial institution (i.e. HIJ Bank) has one or more offices, branches, ATMs, etc. from which its customers may withdraw cash. However, to expand its footprint, HIJ Bank seeks to provide its customers with the capability of withdrawing money from their bank accounts through authorized retail outlets widely available. Generally, only third party providers, which platforms are integrated into M-Commerce server 16 may provide cash withdrawal transactions using the technology of the present invention.

[00200] In this exemplary cash disbursement transaction, a customer, who preferably already has an account with a designated financial entity, such as HIJ Bank, engages the retailer 10 to withdraw money from his/her financial account, as at operation 550. In a preferred embodiment, cash withdrawal transactions are performed using a SIM application menu by retailers that have authorized electronic wallet permissions and SIM security. Characteristics are as earlier described.

[00201] Here, the retailer 10 selects option “(j) HIJ Cash Withdrawal” from the SIM menu. This menu requires the retailer 10 to input, for example, the customer’s unique HIJ Bank identifier (i.e. customer’s bank account number), the withdrawal amount, the retailer’s M-Commerce server identification number (M-PIN), and the customer’s wireless device number. Once the retailer 10 has inputted the prompted information, the application on the retailer’s wireless device 12 displays all the inputs for accuracy confirmation, whether either via “cancel” or “redo” options.

[00202] Upon confirmation of the prompted information details by the retailer 10, the SIM application constructs an encrypted cash withdrawal short message service (SMS) containing the entered data, and sends the message to a SMS center 24, which in turn routes the withdrawal message to the GSM network 14 and on to the M-Commerce server 16. Preferably, the totality of entered data include the customers bank account number, withdrawal amount, the retailer’s M-PIN, the customer’s wireless device number, the retailer’s MSISDN, and the transaction type (i.e. HIJ Cash Withdrawal option (j)).

[00203] From the entered data, the M-Commerce server 16 determines that the cash withdrawal message is a withdrawal transaction, decrypts the message, and authenticates the retailer’s 10 details on the e-Wallet server (operation 552). The M-Commerce server 16 then initiates a cash

withdrawal request (operation 554) to the billing platform of HIJ Bank (not shown) through the third party billing server 600.

[00204] At operation 556, the decisional issue is whether a valid customer's bank account exists. Here, the billing platform of HIJ Bank verifies that the customer's (checking, savings, money market, etc.) account is a valid one by matching the customer's bank account details in the withdrawal request with a bank account database. If no matching data is found, HIJ Bank's billing platform notifies the third party billing server 600 of the mismatch (operation 558). The third party billing server 600 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer via device 12, advising of the failure of the submitted request (operation 560). Alternatively, if the customer's MSISDN identifier was earlier provided, the M-Commerce server 16 also sends a notification SMS message to the customer (via a wireless device), informing that the submitted request failed.

[00205] On the other hand, if the customer's bank account is verified as a valid account, then the next decisional issue is whether sufficient funds exist in the customer's financial account to cover the desired withdrawal amount (operation 562). If not, the third party billing server 600 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer via device 12, advising of the failure of the submitted request (operation 560). Alternatively, if the customer's MSISDN identifier was earlier provided, the M-Commerce server 16 also sends a notification SMS message to the customer (via a wireless device), informing that the submitted request failed.

[00206] However, if there are sufficient funds in the customer's bank account, the HIJ Bank platform sends a notification SMS message to the customer (via a wireless device), advising of the impending withdrawal (operation 564), and prompts the customer to respond with his/her

secret password as to whether to authorize the withdrawal amount (operation 566). If the secret password is not entered, no authorization is deemed to have been provided and HIJ Bank's platform notifies the third party billing server 600 accordingly. The third party billing server 600 notifies the M-Commerce server 16, which in turn sends a notification SMS message to the retailer 10, advising of the failure of the submitted request (operation 560).

[00207] However, if the secret password is entered, authorization of the withdrawal transaction is deemed to have been provided and HIJ Bank's platform cross-references the entered secret password with one in its database to determine if it is a valid one (operation 568). If not, the retailer is notified as described above that the transaction is not successful (operation 560). If the secret password entered is deemed a valid one, HIJ Bank's billing platform (not shown) sends a confirmation message to the third party billing server 600 that the withdrawal request has been accepted for processing, confirming a successful withdrawal (operation 570).

[00208] Next, at operation 572, the third party billing server 600 notifies the M-Commerce server 16, which adds the withdrawal amount to the e-Wallet server 22 of retailer 10. The M-Commerce server 16 also constructs a notification SMS message to the customer's wireless device (operation 574) and retailer (operation 576) confirming that the withdrawal has been successfully posted. Upon receipt of the notification message, the retailer 10 disburses the desired currency to the customer in the withdrawal amount (operation 578).

[00209] Having now described a few embodiments of the invention, it should be apparent to those skilled in the art that the foregoing is merely illustrative and not limiting, having been presented by way of example only. The above embodiments are only to be construed as examples of the various different types of computer systems that may be utilized in connection with the computer-implemented and/or computer-assisted process of the present invention.

Numerous modifications and other embodiments are within the scope of the invention and any equivalent thereto. It can be appreciated that variations to the present invention would be readily apparent to those skilled in the art, and the present invention is intended to include those alternatives.

[00210] For example, as shown and described, the mobile commerce server provides access to a wide range of electronic or digital products and services provided by one or more third party providers that customers may avail themselves of. In some instances, a customer may not be required to possess or have access to a wireless device, such as for the payment of a utility bill. In other instances, such as where a customer seeks to purchase an electronic PIN for online game playing, it is preferable for the customer to have access to a wireless device for delivery of the electronic PIN to the customer.

[00211] Through the use of the third party billing server 600, the present invention is available to one or more customers who may seek alternative disbursement and collection systems other than through traditional bank offices, utility payment offices, ATM machines and the like. As have been earlier described, using the present invention a customer is availed of an extensive network of local, regional or national authorized retailers or merchants through whom they may perform a wide variety of services, such as from payment of a utility bill, subscription to a color ring tone service, to withdrawal of funds, purchasing of event tickets, etc. In addition, these third party billing server services products or services are preferably modular in that each product/service may be enabled or disabled as desired on an individual basis.

[00212] Further, since numerous modifications will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and

described, and accordingly, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

CLAIMS

What is claimed is:

1. A system which provides content and services to a mobile phone service subscriber, said system comprising:
 - an electronic wallet server for:
 - storing a virtual wallet account for a retailer, the virtual wallet account being pre-paid by the retailer and being stored in association with a retailer identification number of the retailer;
 - a mobile commerce server for:
 - receiving an encrypted payment message from a mobile device of the retailer that is a point-of-sale for a mobile phone bill payment being made by a customer to the retailer, the encrypted payment message including a mobile post-paid telephone number of the customer, a billing reference number, a payment amount, and the retailer identification number,
 - decrypting the encrypted payment message,
 - using the retailer identification number, authenticating with the electronic wallet server that the associated virtual wallet account of the retailer contains a sufficient amount of pre-paid funds to satisfy the payment amount;
 - the electronic wallet server further for:
 - holding the payment amount in reserve within the virtual wallet account of the retailer, responsive to the authenticating;
 - the mobile commerce server further for:
 - sending a payment request to a billing platform of a mobile operator providing a mobile service to the customer, the payment request including the mobile post-paid telephone number of the customer, the payment amount, the billing reference number, a payment type, and a unique mobile commerce server transaction number,
 - receiving, from the billing platform, as a response to the payment request either:

(a) a failure notification message when the billing platform determines that the mobile post-paid telephone number included in the payment request is not associated with a post-paid account of the mobile operator, or

(b) an acceptance notification when the billing platform determines that the mobile post-paid telephone number included in the payment request is associated with a post-paid account of the mobile operator, the acceptance notification indicating that payment has been accepted for processing,

forwarding the response to the retailer and the customer, and

when the response is the acceptance notification, instructing the electronic wallet server to deduct the payment amount from the virtual wallet account of the retailer.

2. The system of claim 1, wherein the mobile phone bill payment is a post-paid bill payment transaction.

3. The system of claim 2, wherein the post-paid bill payment transaction involves the customer, who is a subscriber to the mobile service provided by the mobile operator, providing physical currency to the retailer at a physical location of the retailer.

4. The system of claim 1, wherein the mobile device of the retailer that is the point-of-sale is a mobile phone.

5. The system of claim 1, wherein the encrypted payment message is a short message service (SMS) message.