A Subscriber Identity Module (SIM) Chip Bank system and method for enabling users registered in the system to control their financial and telecommunications resources from their mobile device over a mobile communications network. The system combines mobile network providers and financial services through the use of SIM chips without the need for modifying the users' mobile devices or SIM chip installed thereon. A SIM Chip Bank System Operator (SCB-O) regulates data flow between users, banks, mobile communications service providers, SIM Chip Automated teller Machines and SIM Chip Service Providing Machines through a plurality of communications channels. Upon a user connecting to the SCB-O to request a transaction, the SCB-O connects to the appropriate bank to authorize the requested transaction. Upon successful completion, reports are sent back and forth to users confirming the event.
Call SCB-O:
- Voice Call
- Message
- Voice Message
- WEB

Check Mobile Number and Password

Block System

Menu
- Bank Services
- GSM Services
- SCSPM
- Utility Service Providers

Regular Bank Services like Check account, Transfer money, etc.
2. Transfer Money To another SCB-System user.
3. Use of SCB-ATM

Check SCB-System user 1 then transfer Money.
Send Successful message to users.

Send Successful message etc. to UserS.

Special SCB-System Service like Making ADSL Order.

Check SCB-System user 1.
Authorizing the use of SCSPM
SIM CHIP BANK SYSTEM AND METHOD

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority on Jordan Application No. 110/2008, filed on Mar. 9, 2008 and which is herein incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to a Subscriber Identity Module (SIM) Chip Bank System and method. In particular, the system and method enable users to perform various bank operations, to acquire telecommunications services through the use of personal mobile phone with SIM chips installed thereon.

BACKGROUND OF THE INVENTION

[0003] The Internet has revolutionized the manner in which the financial services industry conducts business, in particular by providing customers with permanent accessibility through online and mobile banking business models, which alleviate the need for users to visit their correspondent financial institution. Typically, mobile banking allows customers of a bank to use their mobile devices to access banking services at anytime and from any location through a web browser or using software applications downloaded to the mobile device. Further applications, such as mobile contactless payments or fund transfer between mobile devices, are under development.

[0004] Still, one of the main challenges with current mobile banking systems is a lack of interoperability between different technology standards. In particular, a plurality of protocols is currently being used for mobile banking, thus making it difficult for mobile banking applications to connect multiple banks to provide financial services between accounts held within different banks. Also, given the large variety of mobile devices currently on the market, it is a challenge for banks to offer mobile banking solutions on any type of device. In particular, some devices necessitate Wireless Application protocol (WAP) capabilities to have access to a Uniform Resource Locator (URL) of the corresponding banking server, while others require installation of software applications on the mobile device (thus requiring the device to have relatively large memory capacity) or even complete replacement of the mobile device’s Subscriber Identity Module (SIM) card with extended function SIM cards. In addition, most prior art banking systems require service providers to be equipped with Point-Of-Sale (POS) terminals to confirm the occurrence of a transaction. Other systems necessitate special chips to be integrated in the mobile devices to enable users to remotely access Automated Teller Machines (ATMs), POS terminals and the like, which are in turn equipped with SIM card readers. As a result, the complexity of the overall system is significantly increased. Moreover, strong security concerns arise as financial transactions are executed from remote locations.

[0005] What is therefore needed, and an object of the present invention, is a simplified and efficient SIM chip banking system that enables users to control their financial and telecommunications resources from their mobile device.

SUMMARY OF THE INVENTION

[0006] In order to address the above and other drawbacks, there is disclosed a method for enabling a user of a network enabled mobile device and having an account at a bank to effect financial transactions by directly accessing the account over a wireless network, the mobile device having associated therewith an identifier. The method comprises registering the mobile device with the bank for acquiring mobile payment capabilities, the registering comprising associating the identifier with the account, providing a system operator in communication with the bank, establishing a connection between the mobile device and the system operator, requesting a financial transaction using the account via the connection, the system operator authenticating the user through the identifier and upon authentication directing the request to the bank, and the bank communicating with the user for confirming the request prior to effecting the financial transaction.

[0007] There is also disclosed a system for enabling a user of a network enabled mobile device and having an account at a bank to effect financial transactions by directly accessing the account over a wireless network. The mobile device has associated therewith an identifier and has been registered with the bank for acquiring mobile payment service capabilities, the registration comprising associating the identifier with the account. The system comprises a system operator in communication with the bank, and a connection between the mobile device and the system operator. When the user requests a financial transaction using the account via the connection, the system operator authenticates the user through the identifier and upon authentication directs the request to the bank, the bank communicating with the user for confirming the request prior to effecting the financial transaction.

[0008] Other objects, advantages and features of the present invention will become more apparent upon reading of the following non-restrictive description of specific embodiments thereof, given by way of example only with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In the appended drawings:

[0010] FIG. 1 is a schematic diagram of a Subscriber Identity Module Chip Bank system in accordance with an illustrative embodiment of the present invention;

[0011] FIG. 2 is a detailed schematic diagram of a Subscriber Identity Module Chip Bank system in accordance with an illustrative embodiment of the present invention;

[0012] FIG. 3 is a flowchart of a method implemented in a Subscriber Identity Module Chip Bank system in accordance with an illustrative embodiment of the present invention;

[0013] FIG. 4 is a flowchart of financial transaction process implemented in a Subscriber Identity Module Chip Bank system in accordance with an illustrative embodiment of the present invention;

[0014] FIG. 5 is a schematic diagram of a Subscriber Identity Module Chip Bank system Automated Teller Machine in accordance with an illustrative embodiment of the present invention; and
FIG. 6 is a schematic diagram of a Subscriber Identity Module Chip Service Providing Machine in accordance with an illustrative embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

The present invention is illustrated in further details by the following non-limiting examples.

Referring now to FIG. 1, and in accordance with an illustrative embodiment of the present invention, a Subscriber Identity Module (SIM) Chip Bank system (SCB-system), generally referred to using the reference numeral 10, will now be described. The SCB-system 10 comprises a SIM Chip Bank System Operator (SCB-O) 12 in communication with a plurality (illustratively two (2)) of users as in 14, 14, banks as in 16, 16, and wireless communication network providers (e.g. operator systems using the Global System for Mobile communications (GSM) standard) as in 18, 18, for enabling the users as in 14, 14, to remotely effect financial transactions as well as access telecommunications services through their network enabled mobile devices (references 24, 24, in FIG. 2). In addition, the SCB-system 10 further enables users as in 14, 14, to access banking terminals as in 20, such as an SCB-system Automated Teller Machine (SC-ATM), to perform withdrawals of banknotes, cash transfers, or the like through the GSM networks as in 18, 18, using the mobile devices 24, 24. The system 10 further allows communication with SIM Chip Service Providing Machines (SCSPMs) as in 22, which provide users with a plurality of services such as beverage and food vending or fuel pumping.

Referring now to FIG. 2 in addition to FIG. 1, the mobile devices 24, 24, illustratively include cellular phones, Personal Digital Assistants (PDAs), smart phones, and the like, which are equipped with a smart card (not shown) comprising a SIM chip (not shown). The SIM chip is programmed to retain unique information associated with each mobile device 24, 24, and the corresponding user 14, 14, such as personal identification information, financial account information, and customer information. To access services of the SCB-system 10, the user 14, 14, illustratively registers with the SCB-O 12 for the services by registering the mobile device 24, 24, and the unique identity associated with the device’s SIM chip (for example, the MSISDN associated with the SIM card). This advantageously enables users as in 14, 14, to control their financial and telecommunication resources via their personal mobile device as in 24, 24, without having to modify either the mobile device as in 24, 24, or the SIM chip.

Referring now to FIG. 2, the SCB-O 12 illustratively comprises an authentication system 26, an automatic answering system 28, such as an Interactive Voice Response (IVR) system, a customer service manager system 30, a services risk monitoring system 32 and an intra-connection services system 34, all of which are connected via suitable communications means (not shown) such as a local area network (LAN) or the like. The authentication system 26 illustratively receives incoming communications (e.g. voice calls over GSM call lines as in 36) from the mobile devices as in 24, 24, of users 14, 14, wishing to access the services. After verifying the identity of the mobile devices as in 24, 24, the authentication system 26 diverts (via a switch or the like, not shown) the incoming calls to the appropriate system. Illustratively, if the user 14, is not successfully authenticated (i.e. the mobile device 24, is not registered), the call is directed to the customer service manager system 30, which handles customer service issues (e.g. unauthorized access, troubleshooting, etc.) arising in the SCB-system 10. For this purpose, the customer service management system 30 illustratively comprises a plurality of SCB-O application servers (not shown) and is connected to an SCB-O customer database 38 having stored therein information related to users as in 14, 14, registered with the system 10. Alternatively, if the user 14, 14, is successfully authenticated (i.e. the identity associated with the device’s SIM chip matches information stored in the SCB-O customer database 38), the call is transferred to the IVR system 28. The IVR system 28 illustratively comprises a plurality of IVR servers (not shown) and is connected to an IVR repository database 40, which contains information presented to customers as in 14, 14, for directing the latter to the requested service, as discussed in further detail herein below.

Still referring to FIG. 2, once the users 14, 14, have been authenticated and directed to the requested service, the intra-connection services system 34 is used to direct the flow of transactions and orders via a router (not shown) between the banks as in 16, 16, the GSM providers as in 18, 18, the SC-ATM 20, the SCSPM 22 and the authorized users as in 14, 14. Illustratively, transactions and orders are transmitted by the intra-connection services system 34 to the banks as in 16, 16, and GSM providers as in 18, 18, over secure leased Internet connections as in 42 (e.g. using a Secure Sockets Layer (SSL) protocol) or any other suitable means of connection and/or the SC-ATM 20 and/or SCSPM 22 via the GSM call lines as in 36. Security is further implemented by the services risk monitoring system 32, which monitors transactions effected by the users as in 14, 14, to block and prevent fraud.

Still referring to FIG. 2, the banks as in 16, 16, illustratively each comprise a bank integration services system 44, which communicates with the intra-connection services system 34 of the SCB-O 12 to receive transaction orders and respond with the requested transactions. Illustratively, each bank integration services system 44 comprises an extra integration system 45, which is part of the integration process performed by the bank 16, 16. For this purpose, once transactions and orders are received from the SCB-O 12 via the communications as in 42, each extra integration system 45 establishes a communication channel (or Confirmation Request) 43 between a bank 16, 16, and a mobile device 24, 24, of a user 14, 14, wishing to access the services. The communication is illustratively through any suitable communication means (e.g. IVR, Short Message Service (SMS), or Multimedia Messaging Service (MMS)) and provides a customer 14, 14, contacted by a bank 24, 24, with a choice between confirming, modifying or cancelling the transaction order prior to processing thereof.

Still referring to FIG. 2, each bank 16, 16, further comprises a customer services management system 46 connected to a local SCB-O customer database 48 that holds customer information. The customer services management system 46 illustratively retrieves the stored customer information to identify a user 14, 14, requesting a specific financial transaction, as relayed by the SCB-O 12. Upon identifying and authenticating the user 14, 14, transactions and/or other services to the corresponding financial account of the user 14, 14, are then issued by the bank 16, 16. The bank 16 (or alternatively the bank 16) further comprises a customer data integration and registration system 50 that allows the bank 16, to register new users as in 14, 14, upon request.
from the customer services management 30 of the SCB-O, for example). A core bank integration system 52 is further provided at the bank 16, in the event where the banks 16, 16, are linked via a financial network 54 that enables direct financial transactions and services between financial accounts held in both banks 16, 16, as will be discussed further herein below.

[0023] Still referring to FIG. 2, the GSM operator systems as in 18, 18, illustratively each comprise a GSM operator integration services system 56, which communicates with the intra-connection services system 34 of the SCB-O 12 to receive transaction orders and respond with the requested transactions. For example, the GSM operator systems as in 18, 18, obtain customer information associated with the users as in 14, 14, and assess the GSM number validity of the mobile devices as in 24, 24. Similarly to the financial transaction systems as in 16, 16, the GSM operator systems as in 18, 18, illustratively comprise a customer services management system 58 connected to a local SCB-O customer database 60 for providing requested services to authenticated users as in 14, 14. The GSM operator systems as in 18, 18, further comprise a customer data integration and registration system 62 that similarly allows to register new customers as in 14, 14.

[0024] Still referring to FIG. 2, the SC-ATM system 20 and the SCSPSM 22 similarly illustratively comprise a GSM operator integration services system 64, which communicates with the SCB-O 12 to obtain transaction orders through voice and visual validations for example, a customer services management system 66 connected to a SCB-O customer database 68 and a customer registration system 70, all of which perform functions similar to the functions of the customer services management system 58, the SCB-O customer database 60, and the customer data integration and registration system 62 described herein above.

[0025] Referring now to FIG. 3 in addition to FIG. 2, provided the GSM provider system 18, 18, is affiliated with the SCB-system 10, there is no need for a user 14, 14, to replace or modify the SIM chip currently installed on the mobile device 24, 24, as the SCB-system 10 allows any SIM chip to be registered in the system 10 regardless of the type of mobile device 24, 24, used. Illustratively, upon registration with the SCB-system 10 through the bank 16, 16, that the user 14, 14, is affiliated with, the SIM chip, which is illustratively either pre-paid and/or post-paid, is associated with the financial account held by the registered user 14, 14, at the bank 16, 16. Illustratively, the unique mobile number associated with the mobile device 24, 24, and stored on the SIM chip is used to identify the user 14, 14, at the SCB-O 12 (together with an associated password, for example a number of digits such as a PIN, and/or letters, and/or voice recognition). This unique identity ensures that the user 14, 14, can securely access the services provided by the system 10. In this manner, a SIM chip may illustratively be identified with the same unique identification at the SCB-O 12, the banks as in 16, 16, and the GSM providers as in 18, 18.

[0026] Still referring to FIG. 3 in addition to FIG. 2, more than one mobile phone number may also belong to the same user 14, 14, and mobile device 24, 24, and in this case, the user holds more than one SIM chip, with each SIM chip associated with a unique mobile phone number. Each mobile phone number is 10 then subsequently identified by the SCB-O 12 and associated to the financial account of the user 14, 14. Accordingly, more than one SIM chip may be assigned by the SCB-system 10 to a single account (as a given user may have one or more mobile phones with unique SIM cards in his possession), with the degree of access granted by any number of SIM chips being pre-determined. In this manner, the user 14, 14, would illustratively be provided access to varied services (e.g. effect different financial transactions as described herein above) depending on the smart card and associated SIM chip installed on the mobile device 24, 24.

For example, extra SIM chips may be allowed to connect to the services of the SCB-system 10 using the main identification yet be limited in function to a predetermined set of transactions (e.g. allowed to receive payment reports only but having no access to other services). Updated detailed financial and GSM information corresponding to a given identity is illustratively made readily available and synchronized in the SCB-system 10 through the leased line connections as in 42 between the SCB-O 12, the banks as in 16, 16, and the GSM operator systems as in 18, 18.

[0027] Still referring to FIG. 3 in addition to FIG. 2, a method 100 for handling financial transactions between registered users (references 14, and 14, in FIG. 1) according to an illustrative embodiment of the present invention will now be described. Illustratively, a user 14, having an active financial account held with a bank 16, providing SCB services connects to the SCB-system 10 at 102 using the unique identity (i.e. the mobile phone number) associated with the registered SIM chip. The connection is illustratively implemented by the mobile device 24, initiating a communication at 104 with the SCB-O 12 using the GSM call line 36 to dial the publicly known customer service number of the SCB-O 12. The communication is a combined voice and data communication and may be in the form of a voice call, a text message using the SMS protocol, a voice message, a call or message initiated on the mobile device 24, via the Internet, or an email. Once the communication (illustratively a voice call) is established, the customer authentication system 26 within the SCB-O 12 checks at 106 the mobile phone number associated with the SIM chip of the device 24, to identify whether the user 14, desiring to access the services of the SCB-system 10 is registered in the SCB-system 10 with the SCB-O 12. If the user 14, is not registered, the system 10 blocks the device 24, from accessing the services at 108 and the call is directed to the customer services management system 30 (as discussed herein above). Otherwise, the customer authentication system 26 transfers the call to the IVR system 28, which illustratively responds with pre-recorded or dynamically generated audio and presents at 110 the mobile device 24, with a menu of potential financial transactions available using the account to further direct the user 14, on how to process and enable selection (illustratively using a keypad comprised in the mobile device 24,) of a desired transaction.

[0028] Still referring to FIG. 3 in addition to FIG. 2, a list of possible transactions is illustratively detailed in the menu presented to the mobile device 24, and comprises bank services, GSM services, services provided by the SCSPSM 22 and services provided by other utility service providers (e.g. water or electricity providers). Examples of bank services (provided at 112, and 112,) include regular bank services, such as obtaining financial account details (e.g. bank balance, line of credit, mortgage), and extended bank services such as bill payment, fund transfers to any other account held in the bank 16, macro or micro person-to-person payments among users as in 14, 14, credit services payments, or access to SC-ATMs as in 20. Examples of GSM services (provided at 114) include detailed calling information for the mobile device.
Referring now to FIG. 4 in addition to FIG. 2, in order to request a transfer of funds from a first user 14, to a second user 16, user 14, illustratively contacts the SCB-O 12 at 202 (and connects thereto using its unique ID number and password). The SCB-O 12 then verifies the ID number and password provided by the user 14, to ensure that the user is currently registered with the system 10 and has an active status. Once the user 14, has been authenticated, he SCB-O 12 contacts the bank 16, to which user 14, belongs to fetch the user’s banking details as well as to request at 204 either a fund transfer from the financial account of user 14, to a financial account held by the SCB-O 12 in the same bank 16, or alternatively a fund holding from the financial account of user 14, for subsequent settlement with the SCB-O 12. Upon receiving this request, the bank 16, (after contacting the user 14, via the extra integration system 45 to confirm, change, or cancel the transaction order, as mentioned herein above) either accepts or refuses the transaction and, upon approval of the latter, processes (using for example a suitable workstation, not shown) and confirms the transaction to the SCB-O 12 at 206. At 208, the SCB-O 12 then contacts the financial institution 16, to which user 14, belongs (after having ensured that user 14, is currently registered within the system 10) to issue an order to debit the SCB-O financial account and credit the financial account of user 14, if no financial account exists for the SCB-O 12, the financial institution 16, instead deposits the funds in the financial account of user 14, and subsequently requests settlement from the SCB-O 12. Upon completion of the transaction, bank 16, sends at 210 a confirmation message of success (or alternatively failure) to the SCB-O 12, which subsequently reports the confirmation to both users 14, 14, at 212 and 214 respectively.

Still referring to FIG. 4 in addition to FIG. 2, if a financial network 54 has been implemented between the banks 16, 16, the need for a correspondent financial account held by the SCB-O 12 can be alleviated and the fund transfer transaction described herein above may be processed directly between the banks 16, and 16, by moving funds from the sender’s account to the receiver’s account over the network 54. In this case, the SCB-O 12 solely forwards the fund transfer requests and transaction confirmation message.

Referring now to FIG. 5 in addition to FIG. 2 and FIG. 4, the system 10 enables users as in 14, 14, to access a SC-ATM 20 connected to the SCB-system 10. Illustratively, the SC-ATM 20 is implemented as a standard ATM machine modified to include a registered SIM chip 72 having assigned thereto a unique ATM identifier or ID number 74 in the SCB-system 10, an intercommunication device (intercom) 76 and optionally a camera 78 for receiving calls from the SCB-O 12 and providing visual confirmation (e.g. by initiating a third generation (3G) mobile phone video conference) of the identity of a user 14, 14, in relation to a requested service. Similarly to requests for financial transactions, a user 14, requesting the use of a particular SC-ATM 20 illustratively connects to the SCB-O 12 at 202 in order to have access to the SC-ATM 20. The SCB-O 12 in turn verifies the identity of user 14, and upon positive authentication, the IVR system 28 within the SCB-O 12 queries the user 14, for the ID number 74 of the SC-ATM 20. The SCB-O 12 then connects the user 14, to the specific SC-ATM 20 at 216 by opening via the intercom 76 and camera 78 and for a predetermined time interval a live visual and vocal channel connection (may be recorded for security and legal purposes) between the user 14, and the SC-ATM 20. The user 14, then initiates a transaction, such as a request for withdrawal of banknotes, from the SC-ATM 20. If the SC-ATM 20 belongs to the bank 16, to which user 14, is affiliated, the SCB-O 12 connects to the bank 16, at 204 to request approval of the transaction, upon which approval the financial account of user 14, is debited and the money presented to the user 14, via the SC-ATM 20 in a conventional manner. Alternatively, if the SC-ATM 20 belongs to a bank 16, other than bank 16, the SCB-O 12 illustratively connects to the bank 16, at 208 to request the financial transaction and, upon completion thereof, the bank 16, requests a financial settlement from the SCB-O 12 corresponding to the monetary amount disbursed. A confirmation message that the transaction was successfully completed (or alternatively failed) is then sent at 212 to the user 14, .

Referring now to FIG. 6 in addition to FIG. 2, when the user 14, wishes to connect to a SCSPCM 22, such as a gas pump, the IVR system 28 illustratively similarly queries the user 14, for the ID number (SPM identifier) of the SCSPCM 22 associated with the SIM chip 72 integrated therein. Upon entry of the requested ID number, the SCB-O then connects the user 14, to the specific SC-ATM 20 at 216 by opening via the intercom 76 and camera 78 and for a predetermined time interval a live two-way visual and vocal channel connection between the user 14, and the SCSPCM 22. The SCB-O 12 then queries and confirms the monetary amount to be paid prior to issuing an order to the bank 16, to transfer the requested amount to the SCSPCM 22. Financial settlement between the bank (not shown) the SCSPCM 22 is affiliated with and the bank 16, is illustratively processed in a manner similar to settlements discussed herein above. A confirmation message that the transaction was successfully completed (or alternatively failed) is then illustratively sent to the user 14, .

Referring back to FIG. 1, the SCB-system 10 of the present invention advantageously allows users as in 14, 14, to perform direct and comprehensive bank services and cashless payments directly through their financial account without having to apply for a new bank card. Also, whereas most present art systems require service providers to be equipped with Point-Of-Sale (POS) terminals to confirm the correctness of the transaction, the present invention alleviates the need for such POS terminals to obtain confirmation. Also, the present invention overcomes security concerns by using the unique identification (e.g. mobile phone number) associated with the SIM chip of the mobile device 24, 24. As such, there is no need for special SIM chips to be integrated in the mobile devices as in 24, 24, to provide users as in 14, 14, access to the SC-ATM 20 and/or SCSPCM 22 and any SIM chip (and thus any mobile device 24, 24) may be registered with the system 10. Moreover, the present invention allows person-to-person transactions from any user 14, to another user 14, , even if the other user 14, is affiliated with a different bank 16, 16.

Although the present invention has been described hereinabove by way of specific embodiments thereof, it can be modified, without departing from the spirit and nature of the subject invention as defined in the appended claims.

1. A method for enabling a user of a network enabled mobile device and having an account at a bank to effect financial transactions by directly accessing the account over a
wireless network, the mobile device having associated therewith an identifier, the method comprising:

registering the mobile device with the bank for acquiring mobile payment capabilities, said registering comprising associating the identifier with the account;

providing a system operator in communication with the bank;

establishing a connection between the mobile device and said system operator;

requesting a financial transaction using the account via said connection, said system operator authenticating the user through the identifier and upon authentication directing said request to the bank; and

the bank communicating with the user for confirming said request prior to effecting said financial transaction.

2. The system of claim 1, further comprising installing in the mobile device a smart card comprising a SIM chip programmed with the identifier, the identifier being a mobile phone number.

3. The method of claim 1, wherein said connection is a SSL connection.

4. The method of claim 1, said bank communicating with the user comprising establishing a communication channel between the mobile device and the bank for obtaining at the bank confirmation, modification, or cancellation of said financial transaction.

5. The method of claim 1, wherein said financial transaction is selected from a menu of potential financial transactions available using the account.

6. The method of claim 5, wherein the mobile device comprises a keypad and the user selects one of said potential financial transactions using the keypad.

7. The method of claim 1, wherein said financial transaction is selected from a menu of potential financial transactions provided by an Interactive Voice Response system.

8. The method of claim 1, wherein said financial transaction is between the user and a second user having a second account at a second bank, the method further comprising the bank sending a payment commitment message to said second bank upon completion of said financial transaction.

9. The method of claim 1, wherein said connection is a combined voice and data connection and wherein said confirming said request comprises authenticating a voice of the user.

10. The method of claim 1, further comprising providing a banking terminal interconnected with said system operator and wherein requesting a financial transaction comprises withdrawal of banknotes from said banking terminal.

11. The method of claim 10, wherein said banking terminal is affiliated with a second bank different from the bank and further wherein upon effecting said withdrawal of banknotes from said banking terminal, said second bank requests financial settlement from said system operator.

12. The method of claim 10, wherein said banking terminal is an ATM having an ATM SIM chip installed thereon, said ATM SIM chip programmed with a unique ATM identifier associated with said ATM, said ATM identifier registered with said system operator.

13. The method of claim 10, wherein said banking terminal comprises an intercommunication device and a camera, and further wherein said system operator opens via said intercommunication device and said camera a live visual and vocal connection and wherein said confirming said request comprises confirming an identity of the user via said live visual and vocal connection.

14. The method of claim 1, further comprising a service providing machine in communication with said system operator and wherein requesting a financial transaction comprises transferring funds in payment for a service provided to the user by said service providing machine.

15. The method of claim 14, wherein said service providing machine has a SIM chip installed thereon, said SIM chip having a unique SIM identifier, said SIM identifier registered with said system operator.

16. The method of claim 14, wherein said service providing machine is selected from the group consisting of a food vending machine, a beverage vending machine, and a fuel pump.

17. The method of claim 14, wherein said service providing machine comprises an intercommunication device and a camera, and further wherein said system operator opens via said intercommunication device and said camera a live visual and vocal connection and wherein said confirming said request comprises confirming an identity of the user via said live visual and vocal connection.

18. The method of claim 14, wherein requesting a financial transaction comprises transferring funds from the account to a second account held by said service providing machine at a second bank.

19. The method of claim 18, wherein said second bank is different from the bank, and further wherein upon completion of said transfer of funds, said second bank requests financial settlement from said system operator.

20. The method of claim 1, wherein the identifier enables the user to effect a first predetermined set of financial transactions using the account.

21. The method of claim 20, further comprising associating a second identifier with the mobile device, said registering comprising associating said second identifier with the account, and said requesting a financial transaction using the account comprising said system operator authenticating the user through said second identifier.

22. The method of claim 21, further comprising installing in the mobile device a second smart card comprising a second SIM chip programmed with said second identifier, said second identifier being a second mobile phone number.

23. The method of claim 21, wherein said second identifier enables the user to effect a second predetermined set of financial transactions using the account, said second set being different from said first set.

24. A system for enabling a user of a network enabled mobile device and having an account at a bank to effect financial transactions by directly accessing the account over a wireless network, the mobile device having associated therewith an identifier and having been registered with the bank for acquiring mobile payment service capabilities, the registration comprising associating the identifier with the account, the system comprising:

a system operator in communication with the bank; and

a connection between the mobile device and said system operator;

wherein when the user requests a financial transaction using the account via said connection, said system operator authenticates the user through the identifier and upon authentication directs said request to the bank, the bank communicating with the user for confirming said request prior to effecting said financial transaction.
25. The system of claim 24, further comprising a smart card comprising a SIM chip programmed with the identifier installed in the mobile device, the identifier being a mobile phone number.

26. The system of claim 24, wherein said connection is a SSL connection.

27. The system of claim 24, wherein the bank comprises an integration system for establishing a communication channel between the mobile device and the bank for obtaining the bank confirmation, modification, or cancellation of said financial transaction subsequent to said request.

28. The system of claim 24, wherein said financial transaction is selected from a menu of potential financial transactions available using the account.

29. The system of claim 28, wherein the mobile device comprises a keypad and the user selects one of said potential financial transactions using the keypad.

30. The system of claim 24, wherein said financial transaction is selected from a menu of potential financial transactions provided by an Interactive Voice Response system.

31. The system of claim 24, wherein said connection is a combined voice and data connection and wherein said confirming said request comprises authenticating a voice of the user.

32. The system of claim 24, further comprising a banking terminal interconnected with said system operator and wherein said financial transaction comprises withdrawal of banknotes from said banking terminal.

33. The system of claim 32, wherein said banking terminal is affiliated with a second bank different from the bank and further wherein upon effecting said withdrawal of banknotes from said banking terminal, said second bank requests financial settlement from said system operator.

34. The system of claim 32, wherein said banking terminal is an ATM comprising an ATM SIM chip installed thereon, said ATM SIM chip programmed with a unique ATM identifier associated with said ATM, said ATM identifier registered with said system operator.

35. The system of claim 32, wherein said banking terminal comprises an intercommunication device and a camera, and further wherein said system operator opens via said intercommunication device and said camera a live visual and vocal connection and wherein said confirming said request comprises confirming an identity of the user via said live visual and vocal connection.

36. The system of claim 24, further comprising a service providing machine in communication with said system operator and wherein said financial transaction comprises transferring funds in payment for a service provided to the user by said service providing machine.

37. The system of claim 36, wherein said service providing machine comprises a SPM SIM chip installed thereon, said SPM SIM chip having stored therein a unique SPM identifier, said SPM identifier registered with said system operator.

38. The system of claim 36, wherein said service providing machine is selected from the group consisting of a food vending machine, a beverage vending machine, and a fuel pump.

39. The system of claim 36, wherein said service providing machine comprises an intercommunication device and a camera, and further wherein said system operator opens via said intercommunication device and said camera a live visual and vocal connection and authenticates said unique identifier by confirming an identity of the user via said live visual and vocal connection.

40. The system of claim 36, wherein said financial transaction comprises transferring funds from the account to a second account held by said service providing machine at a second bank.

41. The system of claim 40, wherein said second bank is different from the bank, and further wherein upon completion of said transfer of funds, said second bank requests financial settlement from said system operator.

42. The system of claim 24, wherein the identifier enables the user to effect a first predetermined set of financial transactions using the account.

43. The system of claim 42, wherein a second identifier is associated with the mobile device, said second identifier associated with the account during the registration, and further wherein when the user requests a financial transaction using the account said system operator authenticates the user through said second identifier.

44. The system of claim 43, wherein the mobile device has installed therein a second smart card comprising a second SIM chip programmed with said second identifier, said second identifier being a second mobile phone number.

45. The system of claim 43, wherein said second identifier enables the user to effect a second predetermined set of financial transactions using the account, said second set being different from said first set.

* * * * *