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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 September 2009 (03.09.2009)

PCT

(10) International Publication Number
WO 2009/108066 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/NO2009/000067

(22) International Filing Date:
26 February 2009 (26.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2008 1076 29 February 2008 (29.02.2008) NO

(71) Applicants and
(72) Inventors: **CLOOSTERMAN, Johannes H** [NL/NO]; Hovseterveien 38a, N-0768 Oslo (NO). **ASSAF, Gilles** [NO/NO]; Olaf Bullsvei 5b, N-0765 Oslo (NO).

(74) Agent: **BRYN AARFLOT AS**; P.O. Box 449 Sentrum, N-0104 Oslo (NO).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

WO 2009/108066 A1

(54) **Title**: METHOD AND ARRANGEMENT FOR SECURE TRANSACTIONS

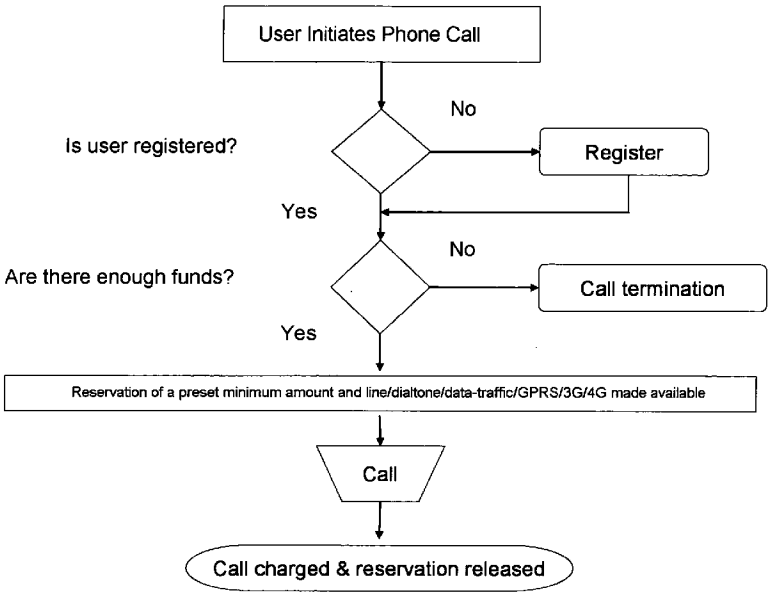

Fig. 1

(57) **Abstract**: A method and arrangement for highly secure payment and processing of payment, utilizing credit card or bank account is disclosed in which the method and arrangement control registration for use of a payment as well as processing through a payment system, using charge card, debit card, payment card, credit card and/or bank account whereas a user utilizes a mobile phone / cell phone, or landline telephone, calls a particular service number or allocated access number hosted by a provider of the processing and payment service.

Description

Method and Arrangement for Secure Transactions

Technical Field

[0001] The present invention relates to a method for a first time registration at a service provider, a method for subsequent use and an arrangement utilising said method for secure transactions utilising telephone.

Background Art

[0002] The last ten years has seen a steady growth in web shopping and internet banking. Following this trend is an increased misuse of credit cards etc. using computers. In many countries internet banking is to be considered a risky business for the user, point of sales or service provider, due to inadequate security systems. Further many of the services provided over internet are not particularly well suited for this; such services may include call-back and other telecom services (pay per call), messaging services consultant services medical services among others.

[0003] The penetration of computers are not as high as it is for telephones, even if landline telephones are omitted, hence there is a need for services on telephones that are secure and easy to use.

[0004] It is known methods for credit card transaction using authentication systems and mobile terminals. From US 2002/0152178 A1 it is disclosed a credit card transaction authentication system using a mobile terminal for performing a work of credit card authentication for a relay system of a VAN company connected between an approval system of a credit card company, which can approve a credit card settlement of the prices, and a transaction approval terminal, which requests credit card transaction approval by means of contactless radio-frequency identification for the mobile terminal containing a transponder therein.

[0005] From US 6,996,547 B1 it is disclosed a method for purchasing items over a non-secure communication channel using a secure communication device. The secure communication device includes a host processor, a secure memory that includes a laser-scribed encryption key, a non secure memory for storing encrypted data. A users´ sensitive data is encrypted within the secure memory using the laser-scribed encryption key and

stored as encrypted data in the non-secure memory. An encrypted credit card number and an encrypted secret key is retrieved from the non-secure memory, the encrypted credit card and secret key are decrypted with the laser-scribed encryption key, the credit card number is encrypted with a session key, and the encrypted credit card number is transferred over the network to a destination such as an internet vendor.

[0006] Still further from GB 2 438 284 A it is known a method for payment authorisation that uses voice biometric where the voice biometric is provided by a telephone or via the Internet.

[0007] All of the methods above have its drawbacks, the US 2002/0152178 A1 describes a one factor systems that lacks necessary security measures to be a candidate for widespread use, further it renders the credit card information/credit card number open to a vendor. Open credit card information stored in databases at a vendor is a huge security problem. Any one who can retrieve data from this database may misuse the credit card information in an easy way.

[0008] In US 6,996,547 B1 it is discussed how to, in a simple manner, facilitate purchasing goods over internet using a mobile terminal for access to the internet. The solution is to pre-load credit card information and authentication information to the memory of the portable device, hence making it easy for the user of the mobile terminal to employ his chosen credit card. The solution necessitates security measures related to the storing of sensitive information on the mobile terminal. However this method does not make the transaction as such a secure business. The method addresses the need to keep sensitive information stored in mobile terminals inaccessible to wrong persons; this is achieved using a laser-scribed encryption key and a decryption algorithm.

[0009] Finally the GB 2 438 284 A teaches how to use biometric voice data to authenticate persons, i.e. map a known voice with a corresponding credit card to be used at a specified user account. According to this document a merchant has to apply either in a written application or over internet to create an account. The teaching of the document is directed towards

professional users such as merchants, hence the registration process is to cumbersome and further includes unnecessary information.

[0010] Hence there is a need for a secure transaction process that facilitates the use of a mobile terminal where authentication and credit card security is ensured.

Disclosure of Invention

[0011] The problems indicated above is met by a method for first time registration at a service provider for a first user where the first user has a telephone and at least a credit card. The method comprises the steps of:

a) The first user calls a service number provided by the service provider from his telephone.

b) Receiving at the service provider a call from the first user.

c) At the receiving party or on behalf of the receiving party performing an ID check of the users' ID-number

d) The receiving party establishes the ID-number as a users' number.

e) The receiving party invites the user to submit his credit card number.

f) The user submits his credit card number.

g) The receiving party receives the credit card number from the user.

h) The receiving party executes a verification check of the received credit card number or is provided with a verification of the received credit card number. If the check turns out to be OK then; the service provider will initiate an encryption algorithm where the credit card number is used as an entry number to the encryption algorithm and the output of the encryption algorithm is an alias number representing the credit card number which is mapped to the user number, or if the check reveals that something is wrong with the credit card number the service provider will reject the user.

[0012] It is also disclosed a method for subsequent use of the service from a service provider for a first user where the first user has a telephone, at least a credit card, and is registered as a user at the service provider and

where the method comprises the steps of:

a) The first user calls a service number at the service provider from his telephone.

b) Receiving at the service provider a call from the first user.

c) At the receiving party or on behalf of the receiving party performing an ID check of the users' ID-number.

d) If the check indicates that the calling party is registered at the receiving party then provide a requested service to the calling party.

[0013] Further it is disclosed an arrangement for first time registration at a service provider for a first user where the first user has a telephone and at least a credit card and where the arrangement at least comprises the following means, means for establishing a call from the first user to a number provided by the service provider from the users telephone, means for performing an ID check of the users' ID-number at the receiving party or means for performing an ID check of the users' ID-number on behalf of the receiving party, means configured to establish the ID-number as a users' number at the receiving party, means configured to execute a verification check or verification of a received credit card number at the receiving party or at credit card company and means configured to initiate an encryption algorithm where the credit card number is used as an entry number to the encryption algorithm and means configured to output an alias number from the encryption algorithm representing the credit card number which is mapped with the user number.

[0014] Still further according to the present invention it is also disclosed other methods for secure payment and processing of payment including a method for registration for use of a payment and processing of payment system using charge card, debit card, payment card credit card and/or bank account where a user utilizes a telephone for calling a particular service number/allocated access number hosted by a provider of the processing and payment service and where the method comprises the steps of:

a) The user calls the provider of the processing and payment service.

b) The provider of the processing and payment service registers the

users ID-number or his call ID.

c) The provider of the processing and payment service requests charge card, debit card, payment card credit card and/or bank account information from the user.

d) The user enters charge card, debit card, payment card credit card or bank account information manually and/or orally using his telephone.

e) The provider of the processing and payment service checks if charge card, debit card, payment card credit card and/or bank account information from the user is valid. If the users' charge card, debit card, payment card credit card and/or bank account is valid then the provider of the processing and payment service is tagging the charge card, debit card, payment card credit card and/or bank account with a unique serial number and/or the users' voice and ID-number, are mapped and stored in database. If the users charge card, debit card, payment card credit card and/or bank account is not valid the provider of the processing and payment service blacklists and/or blocks the users charge card, debit card, payment card credit card and/or bank account in the provisioning of the processing and payment services system after a predefined number of attempts.

f) If the users' charge card, debit card, payment card credit card and/or bank account were valid then the provider of the processing and payment service requests the user to authorize for a single transaction or multiple transactions.

[0015] Other advantageous methods and arrangements will be apparent from the accompanying claims.

Brief Description of Drawings

[0016] To facilitate readability the following description is described with support from the accompanying drawings in which;

[0017] figure 1 discloses a flow diagram in accordance with one aspect of the invention, and

[0018] figure 2 shows an arrangement comprising means configured for secure transactions according to the invention.

[0019] Other advantageously embodiments of the invention will be apparent from the following detailed description and the accompanying claims.

Detailed Description

[0020] In the following the invention will be described with support from the accompanying drawings. Further, the invention will first be described in general terms, thereafter exemplified embodiments will be disclosed, note that the use of first, second, third mode etc. does not indicate any preferred modes.

[0021] Wherever the wording telephone or telephone terminal is explicitly mentioned in the following, it is to be interpreted as any known telephone device that has a kind of keyboard facilitating input of numbers and further where the entered numbers are given unambiguous meanings, i.e. the numbers can be verified and understood by a receiving party. This will then include both mobile phones and landline phones.

[0022] The wording user shall be interpreted in its widest sense as any party, being a single person or a group of persons that tries to use or uses one or more services according to the present invention. In practice the user will normally be a calling party and if accepted he or them will be a customer. The word user may be used interchangeably with the word calling party.

[0023] The wording credit card is used for ease of understanding and to increase readability and any type of credit cards, bonus cards, debit cards, "plastic cards", customer cards, charge cards, payment cards, bank account, customer account or subscription account shall be included in the definition of credit card if nothing else is explicitly indicated. Consequently, the wording credit card number shall be interpreted in the same broad sense that is credit card number includes credit card numbers, bonus card numbers, debit card numbers, "plastic card numbers", customer card numbers, charge card numbers, payment card numbers, bank account numbers, customer account numbers or subscription account numbers. Any person skilled in the art will realise that some of the steps for verification of correctness of credit cards may be superfluous for bank accounts, debit cards, charge cards etc.

[0024] Wherever the wording service provider is written it shall be interpreted as any provider of services or goods that utilizes a method or arrangement

according to the present invention. The wording service provider may be interchanged with the wording receiving party wherever the use of the wording receiving party is more natural. A service provider may provide services on a "real time basis" such as telephone and/or data services or parking services which both necessitates particular solutions due to their nature of real time use and "payment for used amount". A service provider according to the present invention may also provide any type of goods that can be delivered to a customer/user or any type of consultant services. Typical services can be, but is not limited to, medical services such as telephone consultancy, travel services, hotel bookings, air ticket bookings, event bookings, rent of cars, data and telephony services, bank and finance advisory, insurance consultancy, supply of goods such as brown goods, white goods, data equipment etc.

[0025] A-number, telephone number, SIM, IMSI, IMEI number, device's MAC number, (for example; 00:01:E3:B0:C4:C6), in the context of this invention is to be interpreted as an A-number and/or SIM and/or IMSI and/or IMEI number in its traditional meaning as well as any number that unambiguously indicates the number of the calling party to the called party i.e. the service provider. For ease of understanding and readability the wording ID number may also be used in place of A-number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number. The A-number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number may also be used as a customer/user number in the context of the present invention.

[0026] Authenticating authority in the context of the present invention shall be interpreted as any person, tool or authority that is considered as a trusted party by a service provider according to the present invention for authenticating the originator of one or more voice stamps.

[0027] The wording check or checking shall be interpreted generically so as to include the meaning of the words verify or verification in addition to its normal literal meaning.

[0028] Different services may require different levels of security for the user, cheap services such as parking services on a real time basis or telephone

services may not require a high degree of security, whereas services that deal with transfer of valuable goods, services or money transfers may require the highest degree of security. The present invention may be adopted to suit any of these security levels in that it is disclosed a payment processing method, solely using mobile/cell or landline –phones incorporating a choice of multi level security, operating independently from credit card processors and credit card issuers, debit card companies and/or banks.

[0029] On a superficial level the services according to the present invention is a method and arrangement that facilitates use of credit cards for a person having access to a telephone fig 1. The user may use the service by calling a service number; input his credit card details, where the service provider checks the credit card and the ID-number (A-number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number). The user will then be rejected or accepted. If he is accepted he may then start to use the services provided by the service provider.

[0030] In a more secure scenario the service provider may request a voice stamp from the user and in its most secure version the method and arrangement according of the present invention may include that a user delivers a voice stamp with a witness present. The witness may be a notary publicus, a bank officer, a lawyer or any other witness or tool trusted by the service provider such as an automatic code generator.

[0031] One object according to the present invention is to make available safe, single micro payment purchases as well as larger payment transactions for purchase of products or services, using a credit card or bank account through voice instructions using a phone.

[0032] The invention significantly surpasses existing security measurements from established credit card collecting and issuing organizations, including banks.

[0033] By taking advantage of matching and comparing certain parameters; A-Number ID (caller ID) i.e. user phone number/country code, and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number original country of issue and/or SIM and/or IMSI and/or IMEI, and/or device's MAC

number as well original country of issue of credit card or bank organization (ISO code) and making a voice stamp verification. All these parameters must match the user´ ID-number (A-number ID and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number) of the respective country. In the event where a mismatch occurs between any of these parameters or a stolen card is attempted being registered and used by a wrong doer, according to one aspect of the invention the stolen credit card in questions is not only blocked, but the problems are tackled at its roots, it may permanently block the perpetrator as well as the perpetrators phone number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number from entering and/or using other credit cards and/or accounts not yet reported stolen and/or abused. Additionally, the system can send automatic email response to money processing organizations informing of the fraud attempt in progress including the phone number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number of the perpetrator. This chain of measurements virtually eliminates repeated misuse from acknowledged perpetrators and discourages fraud at the outset.

[0034] It is obvious that a first time user of a service must step through a different procedure than in subsequent use, a simple example of a real first time registration may look as follows:

[0035] *First time Credit / bank card registration*

[0036] *02.02 18:13:02 Approving ID-number (i.e. A-nr/Caller ID Country calling from and/or SIM and/or IMSI and/or IMEI number and its country code ID*, and/or device's MAC number*)*

[0037] *02.02 18:13:02 Approving ISO country code identifying credit card country of issue.*

[0038] *02.02 18:13:03 Voice stamp / Voice verification request.*

[0039] *02.02 18:13:18 credit card registration*

[0040] *02.02 18:14:27 credit card approved (first level)*

[0041] As can be seen the first step takes place at 18:13:02 and the final step takes place at 18:14:27, thus the first time registration may be swift and efficient.

[0042] In addition to the possible levels of security one may encounter different scenarios for a first time user, subsequent use, change of credit card details, change of ID-number and deletions of user data.

[0043] The different user scenarios and security levels will be described as a number of equal modes in the following description.

First Mode for Carrying Out the Invention

First time registration

[0044] In the following it is disclosed a mode utilizing a limited degree of security, firstly a registration process is described thereafter subsequent use is described. It shall be noted that even in this mode the method and arrangement according to the present invention is at least as safe as traditional e-commerce (web-shopping).

[0045] A user calls a service number from a telephone. The service provider receives the call from the calling party. The service provider performs checks/verification of the calling party's ID, i.e. ID-number (telephone number, A-number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number). The check is executed by accessing a database that includes tables of number configurations and associated countries as well as a table of registered users; however the latter is not of current interest since it is a first time registration. The service provider is then provided with originating country and the information further enables the service provider to store the calling party's ID-number as a User number/customer number in a data base. If the checks turn out to reveal inconsistent parameters, the user may receive appropriate information. This information may include an invitation to call back or forward to helpdesk.

[0046] While the control and storing routines are performed the calling party may be invited to choose a preferred language or state his/her name, country of residence, prior to further continuation. The result of the optional language choice can be stored in a register that associates the language with the calling party's user number/customer number. This can be a first step of creating a user profile for the calling party at the service provider.

[0047] The user provides the choice of language to the service provider either as a key in choice on his keyboard and/or orally if the service provider is equipped with voice recognition tools.

[0048] The next step may comprise an invitation from the service provider to the user to submit his credit card number (i.e. credit card number includes credit card numbers, bonus card numbers, debit card numbers, "plastic card numbers", customer card numbers, charge card numbers, payment card numbers, bank account numbers, customer account numbers or subscription account numbers).

[0049] The user will respond by entering his credit card number using his telephone keyboard.

[0050] While the calling party enters his credit card number the service provider will forward the credit card number, preferably substantially in real time, to a credit card company or to a data base for verification. Further the calling party will be instructed to enter expiry dates, if existent, and optionally one or more security codes such as CVC codes. All the recorded data will be checked against tables that comprises appropriate data/credit card information. If the check reveals that the credit card user has entered wrong digits or other information, he will be invited to re-enter the number for a predefined number of times, for example three times. If there still is a mismatch after three times the service provider will initiate appropriate actions. These actions may include terminating the call; it may be to inform a credit card company or any other third party to whom it may concern, or it may simply be to inform the calling party that the session will be terminated and that he will be invited to call back or forward to helpdesk. Internally, the service provider may use the provided information, that is, the user ID and the "wrongly entered" number as information for future use.

[0051] If the user has entered correct numbers including optional security check numbers and correct expiration date, if existent, the information will be verified against a register. If it is a traditional credit card that is being checked the ISO country code will be identified, further it will be checked if the card is valid. If the card turns out to be invalid the calling party will be

informed. Further the service provider may store this information; the user will then have a user number/customer number associated with an invalid card.

[0052] If the card turns out to be blocked due to misuse, a number of actions may be initiated. The session with the calling party will obviously be terminated with or without an information message from the service provider. The service provider will preferably map user information with credit card details in his register. The service provider may then use the mapped information for blocking the user for future use for a predefined period of time. If such registration does not take place the service provider will nevertheless, detect future attempts of misuse of blocked credit cards by the checks indicated above. Additionally, the service provider may provide relevant credit card company with user number and/or the number of the credit card. Furthermore, the service provider may also inform governmental institutions such as police about the attempt to misuse the credit card.

[0053] On the other hand, if everything turns out OK, which obviously is the normal scenario, the service provider will preferably encrypt, or, in some other way, transform the credit card number to a serial number. The serial number will then be mapped to the associated user number in a register accessible to the service provider. The number transformation is an important security feature that ensures that any association between mapped personal information and credit card information is inaccessible to a hostile attacker/ a hacker. The step of transformation may take place at this step in the registration procedure or in a previous or subsequent step; the importance of all this is to avoid storing real credit card numbers and particularly to store real credit card numbers associated to real persons.

[0054] After the steps above the user has passed through a first time registration according to one aspect/mode of the present invention. The sequence of steps for registration of a user may vary.

[0055] The steps indicated in this mode of the invention do not ensure an optimal level of security for a user. The credit card checks as such are well taken care of, however there is no personal authentication nor is there any

secure link between user and credit card. This mode of the invention may perfectly well suit services such as provided by parking companies or telephone conversation providers or other services which don't involve expensive goods or services.

[0056] Notwithstanding the apparent cumbersome steps above, in practice it will normally be much faster than what is common within traditional web-shopping.

Subsequent use

[0057] In this section it is described how a registered user may utilize a service according to the present invention exemplified by the first mode. It is assumed that the user calls from the same telephone number as during first time registration. Cases where registered users use new telephones will be discussed in another section. The same applies to cases where users will employ new credit cards or in any other manner depart from "normal procedures".

[0058] A user calls a service number from a telephone. The service provider receives the call from the calling party. The service provider performs checks/verification of the calling party's ID, i.e. ID-number (telephone number, A-number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number). The check is executed by accessing a customer/user-register using the information inherent in the callers ID-number. The service provider is then provided with originating country. If the checks turn out to reveal that something is wrong, the user may receive appropriate information. This information may include an invitation to call back or forward to helpdesk.

[0059] The next step may comprise an invitation from the service provider to the user to submit his credit card number. Alternatively, the user may be invited to use his previously registered credit card details. The user may respond to the invitation to approve use of his registered card by entering a predefined keyboard combination and/or user specific keyboard combination.

[0060] While the calling party enters the requested response, the service provider will forward the credit card number, or more precisely, preferably the serial

number linked to the credit card number, preferably substantially in real time, to a credit card company or to a data base for verification and possibly for a reservation of an amount. If the check reveals that the credit card user has entered wrong keyboard combination he will be invited to re-enter the keyboard combination for a predefined number of times, for example three times. If there still is a mismatch after three times the service provider will initiate appropriate actions. These actions may include to terminate the call; it may be to inform a credit card company or any other third party to whom it may concern or it may simply be to inform the calling party that the session will be terminated and that he will be invited to call back, alternatively to call back or, to forward to a service-desk/help-desk to sort out the problems. The user may simply have forgotten his user specific code. Internally the service provider may use the provided information, that is, the user ID-number and the "wrong entered" number as information for future use.

[0061] If the user has entered correct keyboard combination a preset amount of money will be reserved dependent on the service ordered, provided that acceptance where given by the appropriate instances such as credit card companies. The service is opened to the user. The following steps during the “use of service period” will be strictly dependent on the service provided by the service provider. It is outside the scope of this description to indicate all possible steps necessary during a service since there is a vast combination of services that may utilize the arrangement and method for transfer according to the present invention.

[0062] However, in case of “use per time” and/or Kb/Mb services, one encounter particular problems faced to the prediction of the final costs. Such “use per time” or usage services may include, but are not limited to "telephony services, parking services, consultant services” among others. In case of telephony- or other telecom- service, a scenario may be as follows:

- Calling party enters B-number,
- The inbound cost to the caller is calculated,
- The call forward cost to the called party (B-number) is calculated,
- A set up fee is calculated

- The call is disconnected
- The reservation on the credit card is removed
- Appropriate amount is deducted from the credit card (telephone card, bank card, account, subscriber account etc.)

[0063] In cases where the services are supply of physical goods the prediction steps above will be superfluous, on the other hand one may step through other procedures so as to ensure that correct goods will be delivered etc. The user may go through the steps guided by a telephone voice and he may respond using keyboard combinations and or orally.

[0064] In particular, in cases where it turns out that the credit card number is blocked due to misuse or that it is a stolen card, the service provider will be able to initiate certain counter actions. It is obvious to the person skilled in the art that some of these actions may include those described in the previous section of first time registration. If the card turns out to be invalid the calling party will be informed and the requested services will not be delivered by the service provider. Further the service provider may store this information; the user will then have a user number/customer number (ID-number) associated with an invalid card. If the card turns out to be blocked due to misuse a number of actions may be initiated. The session with the calling party will obviously be terminated with or without an information message from the service provider. The service provider will preferably map user information with credit card details in his register. The service provider may then use the mapped information for blocking the user for future use and or blocking use of the credit card for a predefined period of time.

[0065] Due to the security measures during the first time registration process, it is unlikely that a registered user will attempt to use a stolen and registered credit card. It is however possible to send an alert to the credit card processing company or credit card user, if the rightful owner of the credit card did not have the possibility to block his card before said first time registration process.

[0066] As indicated above in the process of first time registration, the steps indicated in this mode of the invention do not ensure an optimal level of security for a user.

Second Mode for Carrying Out the Invention

First time registration

[0067] As indicated in the previous mode for carrying out the invention the level of security was not optimal. The smartness of the second mode as compared to the first mode is the use of voice stamp for verification of a link between a person and a credit card. Further, use of voice stamp will facilitate some procedures for a method and arrangement for secure transactions. A basic idea behind this mode is that a user more often has access to telephones than to computers, further having access to a phone facilitates use of voice stamp as compared to computers. As a comparison; if a user wants to change IP address he will often have to download a new certificate and step through a first time registration process, each time he wants to utilize an e-commerce service or a bank service, contrary to this, according to a second mode of the present invention, the user will always have the same voice stamp, hence, making a second time registration superfluous in most cases if he changes the telephone number called from.

[0068] The steps for a first time registration may include the following steps;

[0069] A user calls a service number from a telephone. The service provider receives the call from the calling party. The service provider performs checks/verification of the calling party's ID, i.e. ID-number. The check is executed by accessing a database that includes tables of number configurations and associated countries as well as a table of registered users; however the latter is not of current interest since it is a first time registration. The service provider is then provided with originating country and the information further enables the service provider to store the calling party's ID i.e. his ID-number as a User number/customer number in a data base. If the checks turn out to reveal that something is wrong, the user may receive appropriate information. This information may include an invitation to call back or forward to helpdesk.

[0070] While the control and storing routines are performed the calling party may be invited to choose a preferred language for further prosecution. The result of the optional language choice can be stored in a register that associates the language with the calling party's user number/customer number and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number. This can be a first step of creating a user profile for the calling party at the service provider.

[0071] The user provides the choice of language to the service provider either as a key in choice on his keyboard and/or orally. In this second mode the orally delivered choice may be used as a voice stamp for the user. The service provider may invite the calling party to indicate his choice of language by giving him a number of choices and asking him to clearly speak out his choice, e.g. Dutch, French etc. This step may be swapped in the different steps for registering a credit card.

[0072] The next step may comprise an invitation from the service provider to the user to submit his credit card number.

[0073] The user will respond by entering his credit card number using his telephone keyboard and or by spelling it out orally.

[0074] While the calling party enters his credit card number the service provider will forward the credit card number, preferably substantially in real time, to a credit card company or to a data base for verification. Further, the calling party will be instructed to enter expiry dates, if existent, and optionally one or more security codes such as CVC codes. All the recorded data will be checked against tables that comprises appropriate data/credit card information. If the check reveals that the credit card user has entered wrong digits he will be invited to re-enter the numbers for a predefined number of times, for example three times. If there still is a mismatch after three times the service provider will initiate appropriate actions. These actions may include terminating the call; it may be to inform a credit card company or any other third party to whom it may concern or, it may simply be to inform the calling party that the session will be terminated and that he will be invited to call back or forward to helpdesk. Internally the service

provider may use the provided information, that is, the users' ID-number and the "wrongly entered" number as information for future use.

[0075] If the user has entered correct digits including optional security check numbers and correct expiration date, if existent, the information will be verified against a register/database. The credit card ISO country code (country of issue of the credit card) will be identified, further it will be checked if the card is valid. If the card turns out to be invalid the calling party will be informed. Further the service provider may store this information; the provider will then have a user number/customer number identical with or mapped with the ID-number and associated with an invalid card.

[0076] If the card turns out to be blocked due to misuse a number of actions may be initiated. The session with the calling party will obviously be terminated with or without an information message from the service provider. The service provider will preferably map user information with credit card details in his register. The service provider may then use the mapped information for blocking the user for future use for a predefined period of time. If such registration does not take place the service provider will nevertheless, detect future attempt(s) misusing blocked credit cards by the checks indicated above. Additionally the service provider may provide the relevant credit card company with user ID-number and/or the number of the credit card. Moreover, the service provider may also inform governmental institutions such as police about the attempt to misuse the credit card.

[0077] On the other hand, if everything turns out OK, the service provider will preferably encrypt or in some other way transform the credit card number to a serial number. The serial number will then be mapped to the associated user number and the voice stamp in a register accessible to the service provider. In this mode of the inventions it is the mapping between the credit card and the voice stamp that is the most important information as the users' ID-numbers are volatile. The transformation algorithm used in this second mode for carrying out the invention may be the same as the one used in the first mode for carrying out the invention.

[0078] After the steps above the user has passed through a first time registration according to a second mode of the present invention.

[0079] The steps indicated in this mode of the invention ensure a higher level of security for a user than the first mode. In this example the connection between a credit card and a voice is secure, however, there is no explicit verification of the identity of the user, that is, it is not verified that the voice stamp belongs to the identity the user passes on. A person skilled in the art will however realise that the level of security is "one" step above the first mode of the invention. Furthermore, he will realise that misuse of an established customer relationship will be very difficult.

[0080] Notwithstanding the apparent cumbersome steps above, in practice it will normally be much faster than what is common within traditional web-shopping.

Subsequent use

[0081] In this section it is described how a registered user may utilize a service according to the present invention exemplified by the second mode. It is not necessary for the user to use the same telephone as during first time registration. In cases where a user wants to use a new credit card, it will be much simpler than in the case of the first mode as the identity of the user is known and already linked to a voice stamp, therefore, it will be uncomplicated to verify if a persons credit card actually belongs to the actual user claiming to be so.

[0082] A user calls a service number from a telephone. The service provider receives the call from the calling party. The service provider performs checks/verification of the calling party's ID, i.e. ID-number . The check is executed by accessing a customer/user-register using the information inherent in the callers ID-number . The service provider is then provided with originating country. If the checks turn out to reveal that something is wrong, the user may receive appropriate information. This information may include an invitation to call back or forward to helpdesk.

[0083] The next step may comprise an invitation from the service provider to the user to submit his credit card number. Alternatively the user may be invited to use his previously registered credit card. The user may respond to the

invitation to use his registered card by entering a predefined keyboard combination and/or user specific keyboard combination or by orally indicating so. Or the service provider may proceed by taking for granted that the previous registered credit card is the default card for use. If the step includes an oral response from the customer, the service provider may use this oral response as verification for the connection between the user - voice stamp - credit card. In a typical example this step includes; providing a voice stamp from the user, a random PIN code, voice instructed by the service provider, must be repeated and/or entered by the user. The method checks and verifies;

a) the voice-stamp with the called caller ID, and/or
b) the originally registered caller ID and voice-stamp.
c) the voice-stamp with the called caller ID and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number.
d) the originally registered caller ID and voice-stamp and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number.

[0084] The service provider will forward the credit card number or more precisely, preferably the serial number linked to the credit card number, preferably substantially in real time, to a credit card company or to a data base for verification and possibly for a reservation of an amount. In this mode for carrying out the invention it is preferred that the user submits a voice sample in place of user defined keyboard combinations, hence this will make the steps of re-entering codes superfluous. Nonetheless the voice sample will be used as a search entry for search through a customer register. If the search reveals that the credit card user has delivered a wrong voice sample he may be invited to deliver a new voice sample for a predefined number of times, for example three times. It should however be noted that it is very rare that a voice sample delivered from an identified person does not correspond to his registered voice stamp. Hence redelivering of voice samples is therefore unlikely and the option of redelivering may be omitted. If there still is a mismatch the service provider will initiate appropriate actions. These actions may include to terminate the call or service; it may be to inform a credit card company or any other third

party to whom it may concern or, it may simply be to inform the calling party that the session will be terminated and that he will be invited to call back, alternatively, forward to a service-desk/help-desk to sort out the problems. Internally, the service provider may use the provided information, that is, the user ID i.e. ID-number and the "wrong delivered" voice sample as information for future use.

[0085] If the user has entered an acceptable voice sample a preset amount of money may be reserved dependent on the service ordered, provided that acceptance where given by the appropriate instances such as credit card companies. The service is opened to the user. The following steps will be similar to those described for the first mode for carrying out the invention.

[0086] Due to the security measures in the first time registration process it is unlikely that a registered user will attempt to use a stolen and registered credit card. It is however possible to send an alert to the credit card processing company or credit card user if the rightful owner of the credit card did not have the possibility to block his card before said first time registration process.

[0087] A typical example of a real-time transaction for a telecom service providing telephony is disclosed below:

[0088] 01.02 22:20:18 Approving ID-number (A-nr/Caller ID Country and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number) calling from.

[0089] 01.02 22:20:19 Approving ISO country code identifying credit card country of issue.

[0090] 01.02 22:20:35 Credit card reservation and possible Voice stamp request - depending on service

[0091] 01.02 22:20:45 Credit card reservation approved – opening of service.

[0092] 01.02 22:21:07 Calling USA number

[0093] 01.02 22:30:59 Calculating inbound cost to caller

[0094] 01.02 22:30:59 Calculating Call Forward cost to called party (Call Forward)

[0095] 01.02 22:30:59 Calculating setup fee

[0096] 01.02 22:21:20 Voice stamp / auto Voice verification (during call)

[0097] 01.02 22:30:59 Call disconnected

[0098] 01.02 22:31:03 Removing reservation

[0099] 01.02 22:31:08 Deducting amount from credit card or bank account

[00100] As indicated above in the process of first time registration the steps indicated in this mode of the invention does ensure quite a high level of security however not optimal for all user cases.

Third Mode for Carrying Out the Invention

First time registration

[00101] As indicated in the previous mode for carrying out the invention the level of security was not at a maximum for all types of use, even though it was higher than what is common from e-commerce. The smartness of the third mode as compared with the previous mode is the use of an authenticating authority that will authenticate that a voice stamp belongs to the right person. The difference between the second mode for carrying out the invention and the third mode for carrying out the invention lies in the first time registration process. This third mode of the invention renders it almost impossible to misuse a credit card by a person not being the rightful owner of said credit card.

[00102] The additional steps as compared to mode two involves that a person who wants to use a service according to this mode have to deliver a voice stamp under witness of at least one person or other approved tool such as an automatic code generator

[00103] The step may include the following, the user wants to take advantage of a very secure service according to this third mode of the invention, he will then contact a service provider and be instructed to consult a particular office or one or more particular persons. He will further be instructed to bring along accepted identity papers such as passport. At the authenticating office he will be asked to identify himself, thereafter to deliver a voice stamp under witness of at least one person trusted by the service provider. According to one aspect of the invention this trusted person or persons may be trusted by a central or official authority hence giving the voice stamp a very official status. One may imagine that a library of voice stamps can be stored in a secure database. Regardless, the main purpose according to the third mode in order to carry out the

invention is, to make sure that the person who addresses services according to the present invention incorporating secure transactions, is to verify the person he claims to be. Provided that the registration process under witness and with the ID cards is trustworthy, the connection between voice stamp and identity is a 100 percent full-proof.

[00104] After having registered at the registration/authentication authorities, the user may call a service number in the same way as for the first time registration under the second mode for carrying out the invention. Some minor differences are evident, firstly the user will not be invited to deliver a first voice stamp rather he will be invited to deliver a voice sample, where the voice sample is used as a search entry for search in a database comprising authenticated voice stamps. During this registration process the service provider may copy a sample of the voice stamp to his own register or he may access the database comprising the voice stamp each time a person delivers a voice sample. After having registered at the service provider the user will have an "account" similar to the one for the second mode. The only difference is that the user's identity is positively verified and further one may instead of storing voice samples only store a link/pointer to the users authenticated voice stamp.

[00105] The further steps of registering credit card details are very similar to those disclosed in the second mode.

Subsequent use

[00106] Subsequent use after a first time registration at a service provider and after having registered a voice stamp at a trusted authority is very similar to the use indicated for the second mode. The only difference may be that the voice stamp is optionally stored at a remote/central database, hence in stead of accessing a local voice stamp for comparison between a delivered voice sample and a voice stamp the service provider may have to provide the voice stamp to the remote/central database for comparison or the remote/central database provides the service provider with the appropriate voice stamps on requests.

Further advantages and options

[00107] The arrangement and method for secure transaction may as indicated above, accept or reject a user prior to entering the system. Through selective caller identification i.e. ID-number (A-number or caller ID and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number), countries being allowed or not allowed are filtered by accepting or rejecting callers ID-number (caller ID and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number). During the first call in, the rejected caller will receive a voice message, informing of the reject and subsequent blocking, both, in the callers original language and in English. Consecutive call attempts from the rejected caller to enter the system result in busy signals.

[00108] The use of ID-numbers gives extra advantages as compared with traditional services for e-commerce, because, after a user has entered his credit card information, his ID-number, from the calling country, may be compared to the original country of issue of the credit card or bank account. Thereafter, either accepting a transaction for further processing or rejecting. For example; the method determines whether a Norway issued credit card and/or bank account may be used in or for one or more transactions with or to Nigeria, or vice versa. Likewise, the method may block and/or put on hold transfer from a bank account to certain countries and send an email and/or text message such as SMS warning prior to and/or after transfer.

[00109] Finally, disclosed is a test example using a stolen credit card:

[00110] *Attempted registration stolen Credit card.*

[00111] *Rejecting credit card after 3 registration attempts then blacklisting and blocking of:*

[00112] ID-number (A-Number/Caller ID / and/or SIM and/or IMSI and/or IMEI number, and/or device's MAC number) AND Voice Stamp

[00113] *From USA cel/mobile tel number; 0018667176656, (SIM or IMSI or Imei number) 89470010061109003565*

[00114] *02.02 15:47:28 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\200.vox*

[00115] *02.02 15:47:43 Info dtiB1T14 < IsdnDropCall = 0:OK - Dropped inbound call to '0107117939' from '18667176656' (SIM or IMSI or Imei number) 89470010061109003565*

[00116] *02.02 15:47:44 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\210.vox*

[00117] *02.02 15:48:29 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\212.vox*

[00118] *02.02 15:48:34 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\210.vox*

[00119] *02.02 15:49:20 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\212.vox*

[00120] *02.02 15:49:25 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\210.vox*

[00121] *02.02 15:50:10 Info dxxxB1C1 > VoicePlayFile = 0:OK - Playing file C:\VS\Sound\CallnPay2\ENG\212.vox*

[00122] *02.02 15:50:15 Info CALLNPAY2 [4392] Session ended without authorize or sale for 0018667176656, IMSI 89470010061109003565*

[00123] *02.02 15:50:15 Info CALLNPAY2 [4392] Script stopped OK*

[00124] *02.02 15:50:15 Info CALLNPAY2 [4392] Destroyed OK*

[00125] *02.02 15:50:15 Info CALLNPAY2 [4392] Blacklist 0018667176656, IMSI 89470010061109003565*

Claims

1. A method for first time registration at a service provider for a first user where the first user has a telephone and at least a credit card and where the method comprises the steps of:
    a) the first user calls a service number provided by the service provider from his telephone;
    b) receiving at the service provider a call from the first user;
    c) at the receiving party or on behalf of the receiving party performing an ID check of the users' ID-number;
    d) the receiving party establishes the ID-number as a users' number;
    e) the receiving party invites the user to submit his credit card number;
    f) the user submits his credit card number;
    g) the receiving party receives the credit card number from the user;
    h) the receiving party executes a verification check of the received credit card number or is provided with a verification of the received credit card number;
    if the check turns out to be OK then;
        the service provider initiates an encryption algorithm where the credit card number is used as an entry number to the encryption algorithm and the output of the encryption algorithm is an alias number representing the credit card number which is mapped to the user number,
    or
        if the check reveals that something is wrong with the credit card number the service provider will reject the user.
2. A method according to claim 1,
where the method further comprises one or more steps for delivering of at least one voice stamp from the user to the receiving party.
3. A method according to claim 1 or 3,
where the method further comprises one or more steps for delivering of at least one voice stamp from the user to the receiving party under witness of an authenticating authority or utilizing automatic code generator.

4. A method according to claim 3,
   where the receiving party maps the voice stamp to the users other submitted characteristics such as ID-number and credit card number.
5. A method according to any of the previous claims,
   where the method further comprises a step where the receiving party invites the user to choose a preferred language for further communication.
6. A method for subsequent use of a service from a service provider for a first user where the first user has a telephone, at least a credit card, and is registered as a user at the service provider and where the method comprises the steps of:
   a) the first user calls a service number at the service provider from his telephone;
   b) receiving at the service provider a call from the first user;
   c) at the receiving party or on behalf of the receiving party performing an ID check of the users' ID-number;
   d) if the check indicates that the calling party is registered at the receiving party then provide a requested service to the calling party.
7. An arrangement for first time registration at a service provider for a first user where the first user has a telephone and at least a credit card and where the arrangement at least comprises the following means:
   a) means for establishing a call from the first user to a number provided by the service provider from the users telephone;
   b) means for performing an ID check of the users' ID-number at the receiving party or means for performing an ID check of the users' ID-number on behalf of the receiving party;
   c) means configured to establish the ID-number as a users' number at the receiving party;
   d) means configured to execute a verification check of a received credit card number at the receiving party or at credit card company,
   e) means configured to initiate an encryption algorithm where the credit card number is used as an entry number to the encryption algorithm and means configured to output an alias number from the encryption

algorithm representing the credit card number which is mapped with the user number.

8. An arrangement according to claim 10,
where the arrangement further comprises means configured to register voice stamps from the user.
9. An arrangement according to claim 10 or 11,
where the arrangement further comprises means configured to map the voice stamp to the users other submitted characteristics such as ID-number and credit card number.

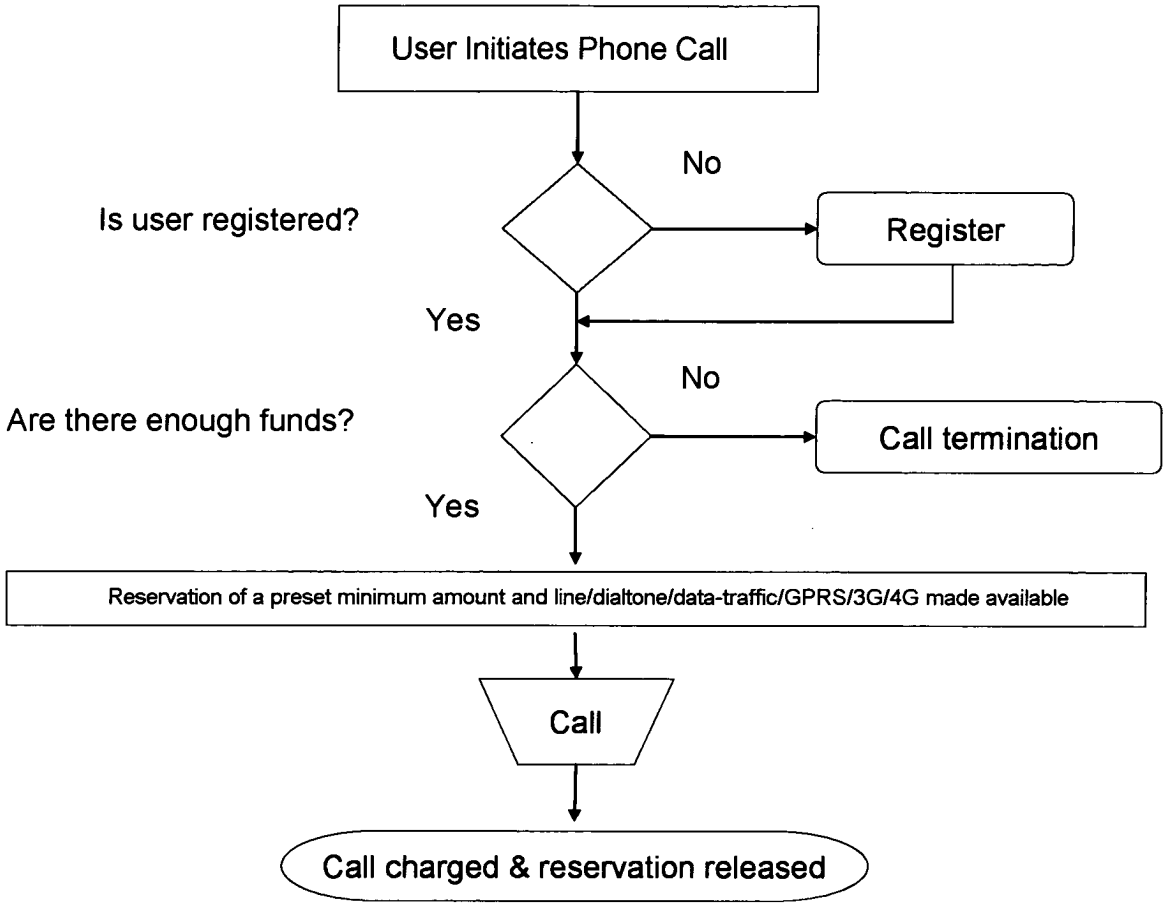
User Initiates Phone Call
Is user registered?
No
Register
Yes
Are there enough funds?
No
Call termination
Yes
Reservation of a preset minimum amount and line/dialtone/data-traffic/GPRS/3G/4G made available
Call
Call charged & reservation released

Fig. 1

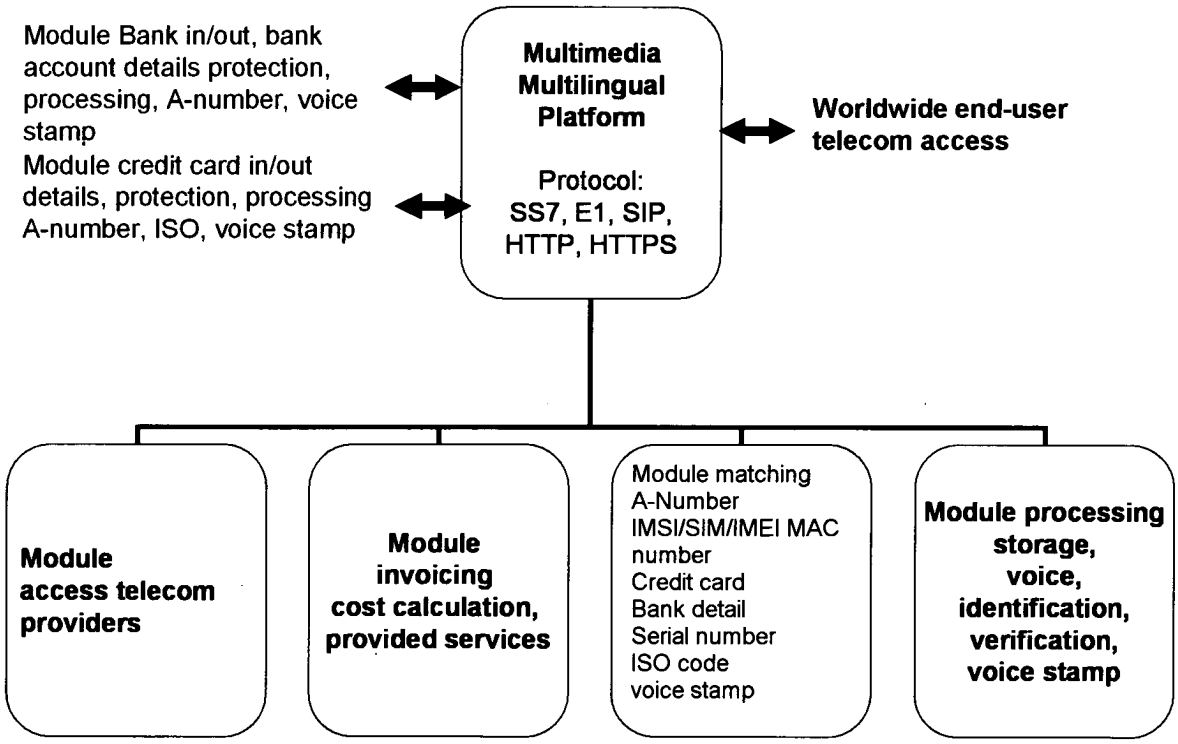
Module Bank in/out, bank account details protection, processing, A-number, voice stamp
Module credit card in/out details, protection, processing A-number, ISO, voice stamp
Multimedia Multilingual Platform
Protocol: SS7, E1, SIP, HTTP, HTTPS
Worldwide end-user telecom access
Module access telecom providers
Module invoicing cost calculation, provided services
Module matching A-Number IMSI/SIM/IMEI MAC number Credit card Bank detail Serial number ISO code voice stamp
Module processing storage, voice, identification, verification, voice stamp

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/NO2009/000067

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/174186 A1 (HOKLAND SEAN [US]) 26 July 2007 (2007-07-26) abstract paragraphs [0008] - [0010], [0020], [0025] - [0028], [0031]; figures 1,2	1-9
X	JP 2002 216181 A (NIPPON SIGNAL CO LTD) 2 August 2002 (2002-08-02)	6
A	abstract	1-5,7-9
X	GB 2 438 284 A (OGDEN JONATHAN NICOLAS; LIMITED VOICEPAY) 21 November 2007 (2007-11-21) the whole document	1-9
X	EP 1 708 473 A (WONG KAMFU [CN]) 4 October 2006 (2006-10-04) the whole document	1-9

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 May 2009	12/06/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kling, Jonas

INTERNATIONAL SEARCH REPORT

International application No
PCT/NO2009/000067

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 371 797 A (BOCINSKY JR RONALD V [US]) 6 December 1994 (1994-12-06) the whole document	1-9
X	US 2006/224508 A1 (FIETZ GUY D [CA]) 5 October 2006 (2006-10-05) the whole document	1-9
A	US 7 127 427 B1 (CASPER ANDREW [US]) 24 October 2006 (2006-10-24) abstract column 2, line 61 - line 64	1-9
A	US 6 996 547 B1 (TUGENBERG STEVEN R [US] ET AL) 7 February 2006 (2006-02-07) the whole document	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NO2009/000067

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007174186 A1	26-07-2007	NONE	
JP 2002216181 A	02-08-2002	NONE	
GB 2438284 A	21-11-2007	NONE	
EP 1708473 A	04-10-2006	WO 2005079050 A1 CN 1914895 A JP 2007519108 T US 2006261152 A1	25-08-2005 14-02-2007 12-07-2007 23-11-2006
US 5371797 A	06-12-1994	NONE	
US 2006224508 A1	05-10-2006	NONE	
US 7127427 B1	24-10-2006	US 2007005445 A1	04-01-2007
US 6996547 B1	07-02-2006	NONE	