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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 May 2010 (14.05.2010)

PCT

(10) International Publication Number
WO 2010/053405 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01) *H04W 12/12* (2009.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/RU2009/000582

(22) International Filing Date:
28 October 2009 (28.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2008143735 6 November 2008 (06.11.2008) RU

(72) Inventor; and
(71) Applicant : **ROZHKOV, Alexander Gennadievich** [RU/RU]; Molostovykh str., 10-1-28, Moscow, 111555 (RU).

(74) Agent: **MIKHAILOV, Alexey Victorovich**; Konyonkov str., 23-211, Moscow, 127560 (RU).

(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, CL, 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, PE, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

[Continued on next page]

(54) Title: TRANSACTION VERIFICATION METHOD, AUTOMATIC TRANSACTION VERIFICATION SYSTEM AND TRANSACTION VERIFICATION UNIT (VARIANTS)

(57) Abstract: The invention offers methods and devices in which a clear-back signal and an answer signal of the subscriber device connected to the automated switched telephone network are used as primary or secondary factor of identification of personality and intentions of the transaction initiator. The invention can be used inter alia for confirmation or verification of transactions initiated by the unauthorized person or by the person authorized by existing authorization factors, by means of the subscriber device of the person authorized to make the transaction. The technical result is the fact that an authorization factor is offered that does not require connection traffic in the automated switched telephone network when such network is used for confirmation or verification of transactions.

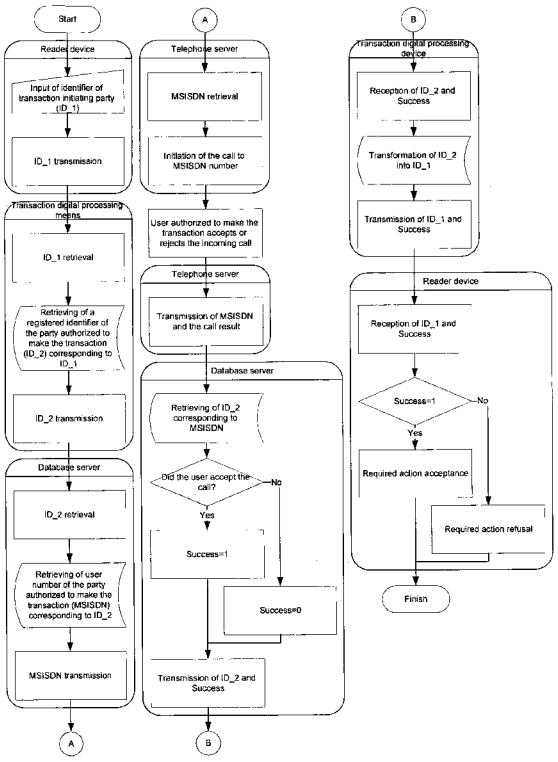


Fig. 8

WO 2010/053405 A1

— *as to the identity of the inventor (Rule 4.17(i))*

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TRANSACTION VERIFICATION METHOD, AUTOMATIC TRANSACTION VERIFICATION SYSTEM AND TRANSACTION VERIFICATION UNIT (VARIANTS)

FIELD OF THE INVENTION

The invention relates to identification means, namely methods and devices for multi-factor verification of transactions made over the telephone.

Transaction parties are generally the first party initiating a transaction, e.g. a bank client, and the second party interested in transaction verification results, e.g. a bank, and the third party performing transaction verification and delivering the result to the second party, e.g. a processing center. In one of the schemes the second and the third parties are combined.

In suggested schemes and devices phone clear-back and answer signals are used as main or additional factors for identification of personality and intentions of transaction initiator.

Inter alia the invention can be used to verify a person's consent to perform an action aimed at transfer of title to the object of transaction in civil circulation. The object of transaction may be material valuables includ money, securities, and goods. Alternatively, the object of transaction can be a delivery permission to a person of information access which is restricted to a limited number of persons; or verification of significant facts, such as authorship of a document, or a person's consent to an action. Thus the invention may be used to authenticate document authorship, and to authenticate a person participating in a process.

The invention may be used to verify payment transactions, transactions in "client-broker" and "client-bank" systems, Internet authorization operations, third-party requests of access to private data, as well as to enable a customer to optionally endorse digital documents with an electronic signature by means of a cell phone.

BACKGROUND OF THE INVENTION

Published U.S. patent application 2003/0061163 A1 herein incorporated by reference in its entirety describes permission verification system and method for credit or debit card use by cardholder during transaction. The minimum system configuration includes a seller's modem, a cardholder's modem, a processing center modem, a database server modem, a private telephone communicator, a database server, and a database. When a credit card is used in a remote sales terminal the seller's modem simultaneously transmits encoded information from the credit card to processing center modem and to the cardholder's modem. As soon as the processing center receives the transaction information from the seller, it transmits the transaction data to the database via modem, private telephone communicator, and database server, and waits for an encoded digital authorization or refusal signal for the transaction from the cardholder. The

cardholder chooses an option in IVR (Interactive Voice Response) menu by pressing the corresponding key on his phone; after that the cardholder's modem transmits the cardholder's choice via a public telephone network simultaneously to the seller's modem, to the processing center modem, and to the database via modem, private telephone switchboard, and database server. The database server saves all transaction data in digital format. If the amount on the debit card is not sufficient, or the credit card limit is exceeded, the processing center is programmed to send a digital signal via modem and public telephone network to the seller's modem about the transaction cancellation, regardless of instructions received from the cardholder via modem.

A shortcoming of aforementioned system is its hardware complexity. It requires two modems on the seller's side for simultaneous communication with the cardholder and the processing center; three modems on the cardholder's side for simultaneous transmission of the cardholder's decision to the seller's modem, to the processing center modem, and to the database; as well as a device transmitting incoming signals via modem to the IVR automatic informer playing back voice files for the cardholder and registering the cardholder's choices. Another shortcoming of the existing system is the considerable amount of time required to coordinate every payment transaction. Transaction completion requires four modem connections, IVR menu playback for the cardholder, and waiting for the cardholder's reply. The cost of transaction verification is increased because of the high per-minute cost of connection in public switched telephone networks.

International publication WO 2006/099081 A2 herein incorporated by reference in its entirety describes a banking account management system and method. When someone requests access to the client's account, the client is notified of such request by a call to the client's number. When the voice connection with the client is being established the system asks the client for the PIN (Personal Identification Number) by playing back the voice file by IVR automatic informer. If the client enters the correct PIN the access to the client's account is granted.

A shortcoming of this system is the high cost of receiving payment transaction verification because of the high per-minute cost of connection in public switched telephone networks, it being necessary for the client to memorize the PIN in order to use the system, as well as the fact that the system cannot be used for small amount payments, because the cost of verification can exceed the transaction amount.

General shortcomings of the existing systems is the long duration of dial-up connection, high requirements to the user's knowledge of verification service infrastructure, dependence of verification results on client's accidental input errors, and verification's being multi-stage and

slow. Existing multi-stage methods can be significantly inconvenient for mobile-phone users on the move e.g. while driving, riding in the subway between stations etc. These shortcomings make multi-stage transaction verification difficult to implement e.g. for verification of routine private operations (the complexity of verification is annoying for users), and for verification of exchange operations requiring instantaneous reaction of a player to the rapidly changing market situation.

So, there still is an unmet demand for means of efficient transaction verification with low per-instance cost requiring minimum participation by the user in the verification process.

SUMMARY OF THE INVENTION

The invention offers methods and devices in which a clear-back signal and an answer signal of the subscriber device connected to the automated switched telephone network are used as primary or secondary factor of identification of personality and intentions of the transaction initiator. The invention may be used inter alia for confirmation or verification of transactions initiated by the unauthorized person or by the person authorized by existing authorization factors, by means of the subscriber device of the person authorized to make the transaction. The technical result is the fact that an authorization factor is offered that does not require connection traffic in the automated switched telephone network when such network is used for confirmation or verification of transactions.

DESCRIPTION OF THE INVENTION

As used herein, "transaction" means a process in which at least two parties participate and which ends in successful or unsuccessful obtaining of a predetermined result. Success or failure to obtain the result are subject to at least one transaction requirement.

As used herein, "transaction requirement" means a provision which can be related to material values or to certain information, and which is subject to verification by means of this invention.

Transaction requirements include, without limitation, the following facts: a person's having a title, authorship, a right to dispose of a material object on behalf of an authorized person, a person's having official authority, a person's having the right to access the information, and a person's willingness to perform a certain action.

A transaction may have several requirements, e.g. a person's having the right to perform an action and a person's willingness to perform a certain action. In such case the transaction result is obtained only after meeting each of the transaction requirements.

As used herein, "transaction result" means an action performed in case of a successful completion of a transaction; said action having been defined prior to the transaction initiation.

Transaction results may be the following actions, without limitation: money transfer from one account to another, gaining access to information, verification of authorship of an electronic document, software execution and activation of any device.

As used herein, "transaction information" means any information related to the transaction parties, transaction requirements, and transaction result. Information on transaction parties includes without limitation a commercial name, a name of a legal entity, a trade mark, a service mark, a service name, a physical person's name. Information on transaction result includes without limitation the following payment information: beneficiary's name, payer's account number, payment currency; information on document: document number and date; information on software: software name and name of the software supplier. Information on transaction requirements includes explanations of the actions which shall be performed to meet the transaction requirement.

As used herein, terms "authorization", "verification", and "validation" are interchangeable and denote a process of checking conformity of an anonymous person with a defined criterion. In case of success an anonymous person is identified as the person characterized by predetermined registration data: name, unique number and scope of authority.

As used herein, "the party authorized to make the transaction", or "the authorized party" means a physical person or a legal entity, or their representatives, or a group of jointly acting persons, or a means by which said persons are represented in electronic environment. The authorized party has the unique identification data formed prior to transaction verification. Such data may include a person's name, a name of a legal entity, or other data making it possible to tell a person from other persons the information on which is used in the invention.

As used herein, "the party initiating the transaction", or "the initiating party" or "the verified party" means a physical person or a legal entity, or their representatives, or a group of jointly acting persons, at whose will a transaction is being initiated. As a specialist will realize, a person's willingness to make a transaction may be expressed by various means and does not necessarily require direct intervention and/or awareness of the initiating party of a transaction being initiated at this party's will. This can be illustrated by mechanical trading systems making trading decisions depending on results of technical analysis of the stock exchange share quotations. As a specialist will realize, "the initiating party" can coincide with "the authorized party" if a transaction is initiated and confirmed by the same person. However "the initiating

party" and "the authorized party' cannot coincide, inter alia, if a transaction is initiated by a dishonest person, or if there is a prior agreement between an authorized party and an honest transaction initiator (for example, if the transaction initiator is a child, and the authorized party is one of the child's parents).

As used herein, "the party verifying transactions", or "the verifying party" is a party by means and by effort of which the transaction requirement verification is performed. The means of transaction verification is an automated infrastructure including a system of interacting software and hardware described below.

As used herein, "the transaction effector party", or "the transaction effector" means a party by means and by effort of which the transaction result is obtained.

Transaction effectors can be, without limitation, the following parties: a bank or a payment system (if the transaction results in a transfer from one account to another), a broker (if the transaction results in a purchase or a sale of securities), a car anti-theft system (if the transaction results in switching the monitoring off), a web or a WAP resource (if the transaction results in authorization at the web- or the WAP resource and/or in gaining access to information content of a web or WAP resource), a rightholder (if a transaction results in a permission to use copyrighted material or software), a physical person or a legal entity (if the transaction results in an endorsement of a document or in permission to use an encrypted file or such property as a personal computer, an automobile, a safe, a DVD).

As used herein, "automated switched telephone network", or "phone network" means at least one public telephone network, such as a stationary public telephone network, or a mobile telephone network, or a combination of the above.

In accordance with the invention the telephone network that the verifying party's device is connected to (verifying party's telephone network), and the telephone network that the authorized party's device is connected to (verified party's telephone network) can be the same network or different networks. Verified party's telephone network is a mobile telephone network. Telephone networks of verifying and verified parties can be connected directly or, not necessarily, by means of one or several telecommunication data transfer channels. In one implementation scheme the telecommunication channel is another telephone network. Whether telephone networks of verifying and verified parties coincide or differ, and regardless of availability, type, quantity and connection sequence of telecommunication channels, the telephone network as a whole provides for addressing a caller and a called party, for

transmission of the caller's address and bidirectional transmission of clear-back and answer signals between a caller and a called party.

In one embodiment of the invention the telephone network uses communication standard selected from the group consisting of GSM (Global System for Mobile Communications), GPRS (General Packet Radio Service), CDMA (Code Division Multiple Access), AMPS (Advanced Mobile Phone System), EV-DO (Evolution-Data Optimized), EDGE (Enhanced Data Rates for GSM Evolution), 3GSM (UMTS - Universal Mobile Telecommunications System, e.g. ITU IMT-2000), DECT (Digital Enhanced Cordless Telecommunications), IS-136/TDMA (Digital AMPS), и iDEN (Integrated Digital Enhanced Network).

In one embodiment of the invention the telephone network is a satellite telephone network.

As used herein, "telecommunication channel", or "data transfer channel" is a means of electronic data transfer (i.e. by electric or radio signals) having at least two end terminals adapted for data transfer between the units connected to them. Telecommunication channel has a predetermined structure and specifications of electric signals and functions in accordance with a physical level protocol, i.e. first-level protocol, according to the seven-level ISO/OSI model. Data transport in telecommunication channel is carried out according to existing protocols of channel, network, transport, session, representation, and applied levels in seven-level ISO/OSI model (see e.g. ISO/IEC 7498-1:1994 and ITU-T Recommendation X.200, 1994).

Data transfer units can be telephone networks or telecommunication channels functioning in accordance with other protocols of physical, channel, network, transport, session, representation, and/or applied levels, or unit elements, in accordance with methods and devices as per the present invention.

In one embodiment of the invention the telecommunication channel uses a physical level protocol selected from the group consisting of V.92 (see ITU-T V.92), IRDA, USB, Firewire, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, Ethernet (see IEEE 802.3 standards), SONET/SDH, GSM radio interface, Bluetooth, IEEE 802.1x Wi-Fi, Etherloop, MTP-1 (Message Transport Protocol), MTP-2, MTP-3.

In a preferred embodiment of the invention the telecommunication channel uses a transport level protocol selected from the group consisting of Ethernet and ISDN.

In one embodiment of the invention the telecommunication channel uses a transport level protocol selected from the group consisting of AEP (AppleTalk Echo Protocol), ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol),

FCIP (Fiber Channel over TCP/IP), FCP (Fiber Channel Protocol), IL (IL Protocol), iSCSI (Internet Small Computer System Interface), LCP (in PPP, Link Control Protocol), NBF (NetBIOS Frames protocol), NBP (Name Binding Protocol), RTMP (Routing Table Maintenance Protocol), SCSI (Small Computer System Interface), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol), UDP Lite, SCTP (Stream Control Transmission Protocol), RSVP (Resource ReSerVation Protocol).

In a preferred embodiment of the invention the telecommunication channel uses a transport level protocol selected from the group consisting of TCP and UDP.

In one embodiment of the invention the telecommunication channel uses a channel level protocol selected from the group consisting of ATM (Asynchronous Transfer Mode), PPP (Point-to-Point Protocol, see e.g. IETF RFC 1661).

In one embodiment of the invention the telecommunication channel uses a network level protocol selected from the group consisting of X.25 (see e.g. ITU-T Recommendation X.25).

In one embodiment of the invention the telecommunication channel uses a telecommunication protocol selected from the group consisting of SS/7 (Signaling System #7, see e.g. ITU-T Recommendation Q.700), and ISDN (Integrated Services Digital Network), WiFi (see e.g. IEEE Standard 802.11).

In one embodiment of the invention the telecommunication channel connecting the telephone network of the verifying party with the telephone network of the verified party functions according to a standard selected from the group consisting of Ethernet, WiFi (see e.g. IEEE Standard 802.11) и Bluetooth (see e.g. IEEE Standard 802.15), ATM (Asynchronous Transfer Mode), SS/7 (Signaling System #7; see e.g. ITU-T Recommendation Q.700), X.25 (see e.g. ITU-T Recommendation X.25), WiMAX (Worldwide Interoperability for Microwave Access, see e.g. IEEE Standards 802.16-802.16e), SCCP (Signalling Connection Control Part), DUP (Data User Part), B-ISUP (B-ISDN User Part), ISUP (ISDN User Part), TUP (Telephone User Part), TCAP (Transaction Capabilities Application Part), SSCOP (Service-Specific Connection Oriented Protocol), H.323, SIP (Session Initiat Protocol), BICC (Bearer Independent Call Control protocol), IS-41, IS-634, CAS, CS1, CS2, R2, CAMEL (Customized Applications for Mobile network Enhanced Logic), INAP (Intelligent Network Application Part), MAP (Mobile Application Part).

In one embodiment of the invention the telecommunication channel uses TCP/IP (Transmission Control Protocol/Internet Protocol, see IETF RFC 1122).

In one embodiment of the invention the telecommunication channel connecting the telephone network of the verifying party with the telephone network of the verified party uses a VoIP (Voice over Internet Protocol) protocol for data transport.

In accordance with the invention, for digital data transmission between telephone networks via telecommunication channels, any suitable digital data transmission can be used – the ones mentioned above as well as the ones known to specialists in this area.

As used herein, "the subscriber address" means a user's telephone number in a public switched telephone network (see Ray Horack, Webster's New World® Telecom Dictionary, Wiley Publishing, Inc., 2007, ISBN 978-0-471-77457-0).

As used herein, "the clear-back signal' means an electric signal normally used in a telephone network when a called party refuses to answer an incoming call (rejects a call signal) after or during receiving an incoming call signal. Thus, a clear-back signal herein does not include a disconnect signal, i.e. a clear-back signal of a caller and/or of a called party sent during a connection.

As used herein, "the answer signal" means an electric signal normally used in a telephone network to inform a caller on a called party's agreement to answer an incoming call after or during receiving an incoming call signal.

For detailed information on telephone network signal system see e.g. GOST (State Standard Specification) 23595-79.

As used herein, "the caller information" in the context of sending the data about a caller by means of the subscriber device of the authorized person, means the set of data unambiguously corresponding to the subscriber address of the caller.

In one embodiment of the invention the caller information is the subscriber address.

In another implementation scheme the caller information is the Caller ID.

In yet till another embodiment the subscriber device of the authorized party includes a means for displaying a predetermined pictogram and/or playing back a predetermined phonogram corresponding to the corresponding user's number or to the Caller ID of the caller. It enables the user to crate easy-to-remember identifiers in order to distinguish the calls of the verifying party from other calls.

As used herein, "the subscriber device of the party verifying a transaction", or "the verifying party subscriber device", denotes a means for gaining access to a public telephone

network providing for transformation of analog and/or digital signals of said network into digital signals compatible with a digital processing device, such as a computer.

The verifying party subscriber device can be a modem. As a specialist will realize, the modem has to be of a type compatible with the telephone system that the verifying party subscriber device is connected to. So, one can use any number of GSM modems, WiFi modems, WiMax modems, 3G modems, 4G modems, satellite modems, radio modems, ADSL modems, ISDN modems, X.25 modems.

As used herein, "the subscriber device of the party authorized to make a transaction", or "the authorized party subscriber device", denotes a mobile means for gaining access to a public telephone network. According to the invention the authorized party has at least the right to use said subscriber device. As a specialist will realize, the authorized party subscriber device has to be of a type compatible with the telephone network that it is connected to.The authorized party subscriber device is a telecommunication device selected from the group consisting of a mobile telephone, a cell telephone, a PDA (Personal Digital Assistant), and a personal computer equipped with a modem.

According to the invention, the authorized party subscriber device can convey information about the caller and is capable of transmitting clear-back and answer signals.

As used herein, "the data storage" means a totality of software and hardware for arranged storage, allocation and modification of data within data structures where each entry unambiguously corresponds to another entry.

In other words, a data storage is a relation database or several interconnected relation databases, as well as means of access to these databases. Database access means includes hardware and software. The hardware includes at least one digital data medium with an electronic access interface and with at least one database present, as well as one or several means of automated digital processing connected to said medium via said interface and equipped with an arithmetic and logic unit.

Data storage software includes at least one database management system (DBMS) providing for allocation, retrieval, and modification of data in said databases. Examples of existing DBMS are MS SQL Server, MySQL, Oracle DBMS, Firebird, Interbase, Sybase, PostgreSQL.

Preferred means of automated digital processing is a database server or several database servers connected by telecommunication channels. The database server or several interacting database servers provide for functionality of said DBMS.

Regardless of the large number of combinations of the above-mentioned means, i.e. specific schemes of database storage, the present invention includes only the functional combinations that are obvious to a specialist, that is one database or several interacting databases managed by one or several DBMS. Said databases are located on one/several digital data medium (media) which in turn is (are) connected to one or several means of automated digital processing.

As used herein, "the reading device" means a device for transforming authorization factor recorded on a medium into electronic analog or digital form for subsequent transmission via the telecommunication channel.

According to the invention, any reading device compatible with the authorization factor medium can be used, such as a magnetic card reader, a barcode scanner, and a radio-frequency identifier reader.

Authorization factor medium can be any data medium, preferably a plastic card with a magnetic strip, a transponder, a plastic card with a microchip. The authorization factor medium can be a body part, such as a finger or an iris, the vocal tract (lips, mouth, tongue, throat, trachea, lungs), the brain (knowledge of token, digital combination, ID).

As used herein, "identification factor of a party initiating a transaction", or "authorization factor", or "identifier of the party initiating a transaction", or "identification data", means any information identifying the person of the transaction initiator.

The authorization factor can be for instance be a biometrical parameter such as a fingerprint, an iris pattern, hand geometry; digital identification means such as a number recorded on a plastic card with a magnetic strip, a letter/number combination (token), a radio-frequency identifier (RFID).

Identification data can be recorded on a digital medium such as a card with a magnetic strip, a card with a microchip, a transponder, a digital optical disk, a barcode. Alternatively identification data are known to the transaction initiator and can be entered into the electronic environment by an input-output device such as a keyboard.

According to the present invention clear-back and answer signals of the subscriber device in the automated switched telephone network are used as authorization factors. They make it possible to identify the party initiating a transaction as the party authorized to make a transaction. The invented authorization factor makes it possible to use for transaction verification just the signal traffic of the automated switched network and does not depend on the signal quality, telephone network capacity, user equipment and the equipment of the verifying party

such as the capacity to form DTMF signals, to perform text message transmission, IVR message playback etc. The invented authorization factor does not require expensive connection traffic in the automated switched telephone network. The invented authorization factor simplifies and accelerates the authorization process by means of the subscriber device. It minimizes the possibility of the user's error typical for existing multi-stage authorization procedures. Technical simplicity of this solution makes it possible to accelerate, and to increase reliability of, authorization process by means of exclusion of connection delays and interruptions caused by data transmission errors in noisy telephone networks.

The invented authorization factor can be used not only as a supplementary authorization factor but as the only authorization factor as well. Implementation of the invented authorization factor as a supplementary authorization factor inter alia increases security of transactions connected with material value title transfers, and decreases the possibility of unauthorized transactions made by an unauthorized person.

In its first aspect the present invention relates to a method for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, comprising the following steps:

(a) providing a subscriber device of the party verifying the transaction having a subscriber address, said device has a capability of transmitting a call signal, recognizing a clear-back signal, and recognizing an answer signal;

(b) providing an automated switched telephone network with said subscriber device of the party verifying the transaction connected thereto; whereby said automated switched telephone network capable of transmiting the call signal, clear-back signal, answer signal, and a caller's address;

(c) providing a subscriber device of the party authorized to make the transaction provided with a subscriber address and having a capability of receiving a call signal and a caller's subscriber address, and can send a clear-back signal, an answer signal, and transmit information about the caller;

(d) providing a data storage comprising a predetermined (i) identifier of the party initiating the transaction, and (ii) an address of said subscriber device of the party authorized to make the transaction associated therewith;

(e) receiving by the party verifying the transaction, of the information about the transaction including the identifier (i) of the party initiating the transaction;

(f) determination by the party verifying the transaction, of the address of the subscriber device of the party authorized to make the transaction, by searching the database storage for the predetermined identifier (i) of the party initiating the transaction, which has to be identical to the identifier of the party initiating the transaction, and by determining the corresponding predetermined address (ii) of the subscriber device of the party authorized to make the transaction; and

(g) initiating a call signal to the subscriber device of the party authorized to make the transaction by means of the subscriber device of the party verifying the transaction;

wherein upon the recognition of an answer signal from the subscriber device of the party authorized to make the transaction, the verifying party identifies the party authorized to make the transaction as giving its consent to make the transaction, and upon the recognition of a clear-back signal from the subscriber device of the party authorized to make the transaction, the verifying party identifies the party authorized to make the transaction as refusing to make the transaction.

In one embodiment, the identifier of the party initiating the transaction is a personal identification number, a login, a password, a bank card number, a radio-frequency identifier (RFID), or a biometrical parameter.

In a preferred embodiment, the radio-frequency identifier is read from a transponder.

In another preferred embodiment the automated switched telephone network includes at least one mobile telephone communication network.

In a more preferred embodiment the mobile telephone communication network uses the GSM standard.

In one embodiment of the present invention, after step (f) and before step (g) an additional message is sent to the subscriber device of the party authorized to make the transaction, the message being selected from the group consisting of a short message service (SMS) message, zero SMS, a multimedia message service (MMS) message, and a message of a bidirectional session transmission of unstructured supplementary service data (USSD); this message is sent through the subscriber device of said mobile telephone communication network which can receive and transmit said SMS, MMS, and USSD messages.

In a preferred embodiment of the invention, the message contains information about the transaction such as the name of a party acting as the transaction effector, the transaction result, the date of transaction initiation, and/or the time of transaction initiation.

In one embodiment of the invention, the message includes information about the transaction selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time, transaction initiation date, transaction beneficiary's name and an electronic digital signature imprint.

In one embodiment of the invention, the subscriber device of the party authorized to make the transaction is a telecommunication device selected from the group consisting of a mobile phone, a cell phone, a personal digital assistant (PDA), and a personal computer equipped with a mobile communication network modem.

In one embodiment of the invention, the call initiated during step (g) is a voice call or a video call.

In one embodiment of the invention, the identifier of the party initiating the transaction is read from a device selected from the group consisting of a magnetic card reader, a barcode scanner, and a radio-frequency identifier reader.

In one embodiment of the invention, information on transactions also includes data selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time, transaction initiation date, transaction beneficiary name, and electronic digital signature imprint.

In one embodiment of the invention, the transaction result selected from the group consisting of a money payment, securities transfer, gaining access to private data, and registration on a web site.

In one embodiment of the invention the subscriber device of the party authorized to make the transaction includes a means of conveying information about the caller selected from the group consisting of phonogram playback means, pictogram indication means, letter/number combination (token) indication means, and a combination of the above.

In a preferred embodiment of the invention the device for conveying information about the caller is used for conveying a phonogram, a pictogram, and/or letter/number combination predetermined for the caller's address. This provides for informing the authorized party on the receipt of the verifying party's call requiring an answer.

In a more preferred embodiment, the subscriber address from which the verifying party makes a call to the subscriber device of the authorized party corresponds to the predetermined transaction information. For example when an incoming call is made from number 555-5555, the mobile phone or a PDA can display a message "Payment of up to $100", and when an incoming call is made from number 555-5556 a message "Payment of $500 to $800" is displayed.

In its second aspect the present invention refers to an automated system for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, comprising:

(a) a first database, the first database arranged to be capable of accumulating of transaction data including identifier of the party initiating the transaction;

(b) a data storage, the data storage includes said first database and at least one second database with predetermined interconnected identifier of the party initiating the transaction, and the subscriber address of a subscriber device of the party authorized to make the transaction;

(c) at least one subscriber device of an automated switched telephone network, the subscriber device can establish connection with a subscriber device of the party authorized to make the transaction, can transmit the caller's subscriber address, and receive clear-back and answer signals,

the subscriber address corresponds to a subscriber device of the party verifying the transaction, and the subscriber device of the party authorized to make the transaction can convey information about the caller and send a clear-back and an answer signal

(d) at least one device for reading the identifier of the party initiating the transaction; and

(e) a transaction digital processing device connected to a reader of the identifier of the party initiating the transaction, and including said data storage and said subscriber device of the automated switched telephone network,

whereby said transaction digital processing device can by means of said data storage (b), accumulate transaction information in said first database (a), and can determine the subscriber address of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and can by means of said subscriber device of the automated switched telephone network, initiate a connection with the subscriber device of the party authorized to make the transaction, can transmit the caller's subscriber address, and receive a clear-back and an answer signal; whereby the subscriber device of the party authorized to make the transaction can convey information about the caller and can send a clear-back and an answer signal.

In one embodiment of the invention, at least one device for reading identifier of the party initiating the transaction is selected from the group consisting of a magnetic card reader, a barcode scanner, and a radio-frequency identifier reader.

In one embodiment of the invention, the information about a transaction also includes data selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time and electronic digital signature imprint.

In one embodiment of the invention, the subscriber device of the party authorized to make the transaction has means to transmit information about the caller through a phonogram, a pictogram, and/or letter/number identifier (token) predetermined for the caller's address.

In one embodiment of the invention the transaction digital processing device includes an arithmetic and logic unit with an input/output device.

In a preferred embodiment of the invention the arithmetic and logic unit is a programmable logic integral scheme.

In one embodiment of the invention the database is an electronic digital medium with an electronic input/output interface.

In a preferred embodiment of the invention the electronic digital medium is selected from the group consisting of a hard-disk drive, a complementary metal-oxide semiconductor (CMOS) chip, and an electrically erasable programmable read-only memory (EEPROM) unit.

In one embodiment of the invention the data storage is a software/hardware complex including a server and a database management system.

According to a third aspect of the invention, there is provided a unit of the automated system for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, which includes the following:

(a) at least one device for transaction information input from the reader of the identifier of the party initiating the transaction;

(b) at least one subscriber device of an automated switched telephone network which is capable of establishing a connection with a subscriber device of the party authorized to make the transaction, convey the caller's subscriber address, and receive a clear-back and an answer signal,

whereby the subscriber address corresponds to the subscriber device of the party verifying the transaction, and the subscriber device of the party authorized to make the transaction can convey information about the caller, and send a clear-back and an answer signal; and

(c) a control device for said at least one subscriber device connected to said at least one transaction information input device (a), and including at least one database containing the

identifier of the party initiating the transaction and the corresponding registered identifier of the party authorized to make the transaction, the registered identifier of the party authorized to make the transaction and the corresponding subscriber address of the party authorized to make the transaction, transaction information including the identifier of the party initiating the transaction and the corresponding transaction status,

whereby said control device for at least one subscriber device can enter into said at least one database, transaction information after the transaction information is received by said at least one transaction information input device and subsequent determination of the registered identifier of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and of the subscriber address of the party authorized to make the transaction according to the registered identifier of the party authorized to make the transaction, can call the subscriber address of the party authorized to make the transaction, and can register the transaction status after receiving a clear-back or an answer signal.

According to a fourth aspect of the invention, there is provided a unit of the automated system for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, which includes the following:

(a) at least one device for transaction information input from the reader of the identifier of the party initiating the transaction;

(b) at least one subscriber device of an automated switched telephone network which can initiate a connection with the subscriber device of the party authorized to make the transaction, convey the caller's subscriber address, and receive a clear-back and an answer signal,

whereby said subscriber device of the party authorized to make the transaction can convey information about the caller, and transmit a clear-back and an answer signal;

(c) a data storage containing predetermined interconnected identifier of the party initiating the transaction, and the subscriber address of the subscriber device of the party authorized to make the transaction,

whereby said data storage can accumulate transaction information including the identifier of the party initiating the transaction, and information on transaction verification result;

(d) a data storage control device which can enter transaction information into said data storage (c) and retrieve from said data storage (c) the subscriber address of the subscriber device of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and

(e) a control device for said at least one subscriber device connected to said at least one transaction information input device (a), and the control device is so arranged that after receiving transaction information from said transaction information input device (a) it enters this information into said data storage (c), retrieves from said data storage (c) the subscriber address of the subscriber device of the party authorized to make the transaction, initiates a connection with the subscriber address of the party authorized to make the transaction by means of the subscriber device of an automated switched telephone network, and after receiving a clear-back signal it enters into the data storage information indicating a negative result of transaction verification, and after receiving an answer signal it enters into the data storage information indicating a positive result of transaction verification.

In one embodiment of the invention the subscriber device of an automated switched telephone network is a GSM modem.

In another embodiment the data storage is a server with a database, and the database storage control device is a database control system.

According to a fifth aspect of the invention, there is provided a method of implementation of clear-back and answer signals in automated switched telephone networks as a transaction requirement which

(a) providing a subscriber device of the party verifying the transaction, the subscriber device has a subscriber address and can initiate a call signal and recognize a clear-back and an answer signal;

(b) providing an automated switched telephone network with the subscriber device of the party verifying the transaction connected thereto, whereby said automated switched telephone network can transmit call, clear-back, answer signals, and caller's address;

(c) providing a subscriber device of the party authorized to make the transaction which has a subscriber address and can receive call signals and the caller's subscriber address, and send clear-back and answer signals;

according to which upon recognition of an answer signal of the party authorized to make the transaction, the verifying party establishes the fact of meeting the transaction requirement, and on recognition of a clear-back signal from the subscriber device of the party authorized to make the transaction, the verifying party establishes the fact of a failure to meet the transaction requirement.

In its sixth aspect the invention refers to a method of implementation of clear-back and answer signals in automated switched telephone networks as a factor of identification of the party initiating a transaction which

(a) uses the subscriber device of the party verifying the transaction which has a subscriber address and can initiate a call signal and recognize a clear-back and an answer signal;

(b) uses an automated switched telephone network with the subscriber device of the party verifying the transaction connected thereto, whereby said automated switched telephone network can transmit call, clear-back, answer signals, and caller's address;

(c) uses the subscriber device of the party authorized to make the transaction which has a subscriber address and can receive call signals and a caller's subscriber address, and to send clear-back and answer signals;

according to which on recognition of an answer signal of the party authorized to make the transaction, the verifying party identifies the party initiating the transaction as the party authorized to make the transaction, and on recognition of a clear-back signal from the subscriber device of the party authorized to make the transaction, the verifying party identifies the party initiating the transaction as a party not authorized to make the transaction.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a flow chart of one of the embodiments of the verification system according to the invention, with the use of a cell phone as a subscriber device of an authorized party.

Figure 2 is a flow chart illustrating embodiment of the invention for verification of transactions in which the medium with the initiating party's identifier is a plastic card with a magnetic strip.

Figure 3 is a flow chart illustrating embodiment of the invention for verification of transactions in which the initiating party is identified in electronic environment by means of an executable program within a "Bank-Client" system.

Figure 4 is a flow chart illustrating embodiment of the invention in the world-wide web to verify transactions the object of which is a fact of authorship of transaction initiator.

Figure 5 is a flow chart illustrating embodiment of the invention for verification of transactions having the requirement of transaction initiator's having rights to use a software product or to access information.

Figure 6 is a flow chart illustrating embodiment of the invention for verification of transactions having the requirement of transaction initiator's authorship in relation to an

electronic document. Figure 6 illustrates the invention implementation both separately and in combination with an electronic signature.

Figure 7 is a flow chart illustrating embodiment of the invention for verification of transactions having the requirement of transaction initiator's having rights to perform an action relating to an automobile.

Figure 8 shows the algorithm of one of the embodiments.

Figure 9 graphically shows parties participating in a transaction using an example of one embodiment for the banking sector.

DESCRIPTION OF PREFERRED EMBODIMENTS

The invention will now be illustrated by reference to the following example.

EXAMPLE 1

TRANSACTION VERIFICATION SYSTEM

As shown in Figure 1, the transaction verification system includes reader device 2 and transaction digital processing device 4 sequentially connected by means of telecommunication channel 3, database 7 connected to transaction digital processing device 4, database server 8 connected to transaction digital processing device 4 by means of telecommunication channel 5, database 13 connected to database server 8, mobile communication network 10 connected to automated switched telephone network 11, which in its turn by means of the verifying party's subscriber device (not shown), is connected to telephone server 12, telephone server 12 is connected to database 8. Transaction initiator 6 in order to work with the system uses user identifier 1 recorded on a medium, and mobile telephone 9 as the subscriber device of the party authorized to make the transaction.

For the sake of simplicity in the present example the transaction initiator coincides with the authorized party, and is the owner of the subscriber device of the authorized party.

User identifier 1 medium (not shown in Figure 1) is a card with a magnetic strip, a transponder, a key to an electronic lock, a radio-key (for instance, a car alarm system transmitter).

User identifier 1 is inter alia a biometrical property of user 6 such as a fingerprint, an iris pattern etc., or a known to the transaction initiator 6 letter/number combination (token) such as a PIN, a login, or a password.

Reader device 2 is inter alia an ATM (Automated Teller Machine), a POS terminal, a lock with an electronic key, a car anti-theft system, an express payment terminal, a biometrical

identification device, or a letter/number or digital combination input device. Reader device 2 can be located in an area open for access by transaction initiator 6 for user identifier 1 input, and at any distance from other elements of the system, subject to maintaining the functionality of telecommunication channel 3.

Telecommunication channel 3 is one or several interconnected wire or wireless communication lines.

Transaction digital processing device 4 is inter alia a personal computer, an industrial computer, or other computing device. Transaction digital processing device 4 can perform the following functions:

(a) to receive user identifier 1 via telecommunication channel 3 from reader device 2;

(b) to send a request to database 7 with the recognition of the identifier of the party authorized to make the transaction based on the identifier of the party initiating the transaction, i.e. on user identifier 1;

(c) to transmit the user identifier of the party authorized to make the transaction via telecommunication channel 5 to database server 8.

Transaction digital processing device 4 can be located separately from database server 8. In this case transaction digital processing device 4 is connected to database server 8 via telecommunication channel 5.

Telecommunication channel 5 is one or several wire or wireless communication line(s). Telecommunication channel 5 does not necessarily include Internet elements and/or other existing telecommunication networks.

Database 7 includes data structures in which the identifier of the party initiating the transaction (i.e. user identifier 1) is unambiguously connected with the identifier of the party authorized to make the transaction.

Database server 8 is a personal computer, an industrial computer, or other computing device. Database server 8 can perform the following functions:

(a) to receive the identifier of the party authorized to make the transaction from transaction digital processing device 4 via telecommunication channel 5;

(b) to send a request to database 13 with the recognition of the subscriber address of the party authorized to make the transaction based on the identifier of the party authorized to make the transaction;

(c) to transmit the subscriber address of the party authorized to make the transaction to the subscriber device of the verifying party 12.

It is assumed that the received subscriber address corresponds to subscriber device 9 of transaction initiator 6.

Subscriber device 9 is a telecommunication device registered in mobile communication network 10 and is a mobile telephone, or a cell telephone, or a personal digital assistant, or a personal computer equipped with a subscriber device having a subscriber address in mobile communication network 10. A mobile telephone can be directly accessed by transaction initiator 6.

Mobile communication network 10 is a cellular or a satellite communication network.

Channel of switched telephone network 11 is a stationary telephone communication network or several such networks interconnected.

Telephone server 12 is one or several modems, a personal computer with a Dialogic telephony card, an industrial computer with a Dialogic telephony card, an intellectual communication platform, or other telecommunication device which can perform the following functions:

(a) to receive the subscriber address of the party authorized to make the transaction from database server 8;

(b) to initiate an outgoing call to the received subscriber address via switched telephone network channel 11;

(c) to wait for an answer to said call;

(d) to disconnect immediately if the called user answers the call;

(e) to transmit subscriber address and the result of said call to database server 8.

Database 13 includes data structures in which the identifier of the party authorized to make the transaction unambiguously corresponds to the subscriber address of the party authorized to make the transaction.

Telephone server, database server 8, and database 13 are located in the same information environment in order to provide for the security of the transactions made.

A system shown in Figure 1 functions as follows. As illustrated in Figure 8, transaction initiator 6 by means of reader device 2 enters the identifier of the party initiating the transaction (hereinafter "ID1"). Reader device 2 transmits ID1 to transaction digital processing device 4. Transaction digital processing device 4 sends a request about ID1 to database 7. Database 7

transforms ID1 into a pre-registered identifier of the party authorized to make the transaction (hereinafter "ID2"), and transmits it to transaction digital processing device 4. Transaction digital processing device 4 transmits ID2 to database server 8. Database server 8 sends a request about ID2 to database 13. Database 13 transforms ID2 into the subscriber address of the party authorized to make the transaction (hereinafter MSISDN), and transmits it to database server 8. Database server 8 transmits MSISDN to telephone server 12. Telephone server 12 initiates a call to mobile phone 9 of user 6. If user 6 rejects the incoming call from telephone server 12, then telephone server 12 transmits the result to database server 8. If user 6 accepts the incoming call from telephone server 12, then telephone server 12 immediately terminates the initiated call and transmits the result to database server 8. If the call is rejected by user 6, then database server 8 sets the Success variable to "0". If the call is accepted by user 6, then database server 8 sets the Success variable to "1". The database server sends a request about MSISDN to database 13. Database 13 transforms MSISDN into ID2 and transmits it to database server 8. Database server 8 transmits ID2 and the Success variable value to transaction digital processing device 4. Transaction digital processing device 4 sends a request about ID2 to database 7. Database 7 transforms ID2 into ID1 and transmits it to transaction digital processing device 4. Transaction digital processing device 4 sends ID1 and the Success variable value to receiving device 2.

EXAMPLE 2

IMPLEMENTATION OF THE TRANSACTION VERIFICATION SYSTEM FOR PLASTIC CARD OPERATIONS IN THE BANKING SECTOR

The scheme of the transaction verification system implemented for verification of operations with a plastic card as a medium for user identifier 1 is shown in Figure 9.

For the sake of simplicity it is assumed that the transaction initiator and the authorized party coincide. Transaction initiator 6 inserts a bank plastic card (a medium for user identifier 1) into the ATM (the reader device 2) located within the Merchant Area, enters the PIN and instructs the ATM to make a cash withdrawal from the transaction initiator's personal account. The ATM via telecommunication channel 3 transmits the card data to the bank processing center (transaction digital processing device 4) located in the Bank Area. Processing center 4 by means of database 7 determines ID2 using received identifier of the transaction initiator 1, and transmits ID2 via telecommunication channel 5 to database server 8. Database server 8 by means of database 13 using the received ID2 determines the subscriber address of the transaction initiator MSISDN. Database server 8 instructs telephone server 12 to make an outgoing call to the subscriber device of transaction initiator 9. Database server 8, database 13, and telephone server

12 are located in Verifying System area. Telephone server 12 with the help of the subscriber device (not shown) connected to a stationary telephone network calls the subscriber device of transaction initiator 9. An automated switched telephone network is connected to mobile communication network 10, to which the subscriber device of transaction initiator 9 is connected. The subscriber device of transaction initiator 6 should have the Caller ID service activated. The transaction initiator sees the number of the incoming call and realizes that the call is sent by the verifying party. By answering the incoming call transaction initiator 6 agrees to make the transaction; by rejecting the call (refusing to accept the call) the user prohibits the transaction.

Thereby, to receive a reply from transaction initiator 6, only the signal traffic of switched telephone network 11 is used, without any usage of a voice communication channel, and the confirmation or the refusal regarding the transaction is conveyed by the answer to the verifying party's call by the transaction initiator, or correspondingly, by the refusal to answer such a call.

For a user to be able to identify 6 different types of authorization requests, database server 8 makes an outgoing call from different subscriber addresses. For example, for a request to make a transaction for the amount of up to 5,000.00 rubles the system makes an outgoing call to the telephone of the transaction initiator from the number +7(495)123-40-00, and for transaction for the amount of up to 15,000.00 rubles the call is made from the number +7(495)123-40-02. The transaction initiator for the sake of convenience can save these numbers in the telephone memory under easily identifiable names, e.g. "A payment of up to 5,000 rubles", "A payment of up to 15,000 rubles" etc. If initiator 6 answers to the incoming call, then telephone server 12 immediately terminates this call. Following that telephone server 12 transmits to database server the status of the call made (whether or not user 6 with the corresponding MSISDN has answered the call). The result of the user's answer after the reverse transformation as shown in Figure 8 illustrating the system algorithm is transmitted to the processing center. The processing center based on the answer received from the subscriber device of transaction initiator 9 instructs the ATM whether to dispense or not, the cash requested by transaction initiator 6.

EXAMPLE 3

As shown in Figure 2 the invented authorization factor can be used in addition to the authorization factor recorded on a credit or a debit bank card, when the transaction initiator withdraws cash from an ATM.

EXAMPLE 4

As shown in Figure 3 the invented authorization factor can be used by a small business company director to endorse the payment instructions for the company's account prepared by the accountant.

EXAMPLE 5

As shown in Figure 4 the invented authorization factor can be used to replace passwords for several WEB resources with one universal password with a mobile confirmation.

EXAMPLE 6

As shown in Figure 5 the invented authorization factor can be used to check whether a transaction initiator has the right to access any information systems, data storages, or any specific data within such storages.

EXAMPLE 7

As shown in Figure 6 the invented authorization factor can be used in addition to an electronic signature for remote endorsement of digital documents by the transaction initiator.

EXAMPLE 8

As shown in Figure 7 the invented authorization factor can be used to verify transactions resulting in switching on an electronically controlled mechanism, for example an electronic lock, a car control system, a computer power-on button, a safe equipped with an electronic lock, a VCR etc.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS

1. A method for verification of the consent of the party authorized to make the transaction to making the transaction by the party initiating the transaction, comprising the following steps:

(a) providing a subscriber device of the party verifying the transaction the device having a subscriber address, abovementioned device has a capability of transmitting a call signal, recognizing a clear-back signal, and recognizing an answer signal;

(b) providing an automated switched telephone network with said subscriber device of the party verifying the transaction connected thereto; whereas said automated switched telephone network is capable of transmiting the call signal, clear-back signal, answer signal, and a caller's address;

(c) providing a subscriber device of the party authorized to make the transaction the device provided with a subscriber address and having a capability of receiving a call signal and a caller's subscriber address, and having a capability of sending a clear-back signal, an answer signal, and transmitting information about the caller;

(d) providing a data storage comprising a predetermined (i) identifier of the party initiating the transaction, and (ii) an address of said subscriber device of the party authorized to make the transaction associated therewith;

(e) receiving by the party verifying the transaction, of the information about the transaction including the identifier (i) of the party initiating the transaction;

(f) identification by the party verifying the transaction, of the address of the subscriber device of the party authorized to make the transaction, by searching the database storage for the predetermined identifier (i) of the party initiating the transaction, the identifier having to be identical to the identifier of the party initiating the transaction, and by determining the corresponding predetermined address (ii) of the subscriber device of the party authorized to make the transaction; and

(g) initiating a call signal to the subscriber device of the party authorized to make the transaction by means of the subscriber device of the party verifying the transaction;

wherein upon the recognition of an answer signal from the subscriber device of the party authorized to make the transaction, the verifying party identifies the party authorized to make the transaction as giving its consent to make the transaction, and upon the recognition of a clear-back signal from the subscriber device of the party authorized to make the transaction, the

verifying party identifies the party authorized to make the transaction as refusing to make the transaction.

2. The method according to claim 1, wherein the identifier (i) of the party initiating the transaction is selected from the group consisting of a personal identification number, a login, a password, a bank payment card number, a radio-frequency identifier (RFID), and a biometrical parameter.

3. The method according to claim 2, wherein the radio-frequency identifier is read from a transponder.

4. The method according to any of the claims from 1 to 3, wherein an automated switched telephone network comprises at least one mobile telephone communication network.

5. The method according to claim 4, wherein the mobile telephone communication network is a GSM network.

6. The method according to claim 5, wherein after step (f) and before step (g) an additional message is sent to the subscriber device of the is party authorized to make the transaction, this message selected from the group consisting of a short (SMS) message, a zero-class SMS message, a multimedia (MMS) message, and a message of the bi-directional session transmission of unstructured data of additional services (USSD), whereas the subscriber device of said mobile telephone communication network can receive and display said SMS, MMS, and USSD.

7. The method according to claim 1, wherein said subscriber device of the party authorized to make the transaction is a telecommunication device selected from the group consisting of a mobile telephone, a cellular telephone, a personal digital assistant, and a personal computer provided with a GSM modem.

8. The method according to claim 6, wherein said message comprising the transaction data selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time, transaction initiation date, transaction beneficiary, and electronic digital signature imprint.

9. The method according to claim 1, wherein during step (g) a voice call or a video call is initiated.

10. The method according to claim 1, wherein the identifier (i) of the party initiating the transaction is read from the device selected from the group consisting of a magnetic card reader, a barcode scanner, and a radio-frequency identifier reader.

11. The method according to claim 1, wherein information on transactions also includes data selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time, transaction initiation date, transaction beneficiary, and electronic digital signature imprint.

12. The method according to claim 1, wherein a transaction is made which is selected from the group consisting of a money transfer, a transfer of securities, confirmation of authenticity of private data, and confirmation of registration at a web site.

13. The method according to claim 1, wherein the subscriber device of the party authorized to make the transaction is used to convey information about the caller, the information selected from the group comprised of a phonogram playback device, a pictogram display device, a letter/number identifier indication device, and combinations of the above.

14. The method according to claim 13, wherein the caller information is presented on the subscriber device of the party authorized as the phonogram, the pictogram, and/or the letter/number identifier predetermined for the caller's address.

15. An automated system for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, the system comprising:

(a) a first database, the first database arranged to be capable of accumulating of transaction data including identifier of the party initiating the transaction;

(b) a data storage, the data storage includes said first database and at least one more database with predetermined interconnected identifier of the party initiating the transaction, and the subscriber address of a subscriber device of the party authorized to make the transaction;

(c) at least one subscriber device of an automated switched telephone network, the subscriber device being able to establish connection with a subscriber device of the party authorized to make the transaction, and transmit the caller's subscriber address, and receive clear-back and answer signals,

the subscriber address corresponds to a subscriber device of the party verifying the transaction, and the subscriber device of the party authorized to make the transaction can convey information about the caller and send a clear-back and an answer signal

(d) at least one device for reading the identifier of the party initiating the transaction;

and

(e) a transaction digital processing device connected to a reader of the identifier of the party initiating the transaction, and including said data storage and said subscriber device of the automated switched telephone network,

whereas said transaction digital processing device can by means of said data storage (b), accumulate transaction information in said first database (a), and can determine the subscriber address of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and can by means of said subscriber device of the automated switched telephone network, initiate a connection with the subscriber device of the party authorized to make the transaction, can transmit the caller's subscriber address, and receive a clear-back and an answer signal; whereas the subscriber device of the party authorized to make the transaction can convey information about the caller and can send a clear-back and an answer signal.

16. The system according to claim 15, wherein at least one reading device for the identifier of the party initiating the transaction is selected from the group consisting of a magnetic card reader, a barcode scanner, and a radio-frequency identifier reader.

17. The system according to claim 15, wherein transaction information also includes information selected from the group consisting of transaction amount, account number, currency, account balance, transaction initiation time, and electronic digital signature imprint.

18. The system according to claim 15, wherein the subscriber device of the party authorized to make the transaction can convey information about the caller by means of a phonogram, a pictogram, and/or letter/number identifier predetermined for the caller's subscriber address.

19. The system according to claim 15, wherein said transaction digital processing device (e) includes an arithmetic and logical device with input/output unit.

20. The system according to claim 19, wherein the arithmetic and logical device is a programmable logical integrated circuit.

21. The system according to claim 15, wherein said data storage (b) is an electronic digital medium with an electronic input/output interface.

22. The system according to claim 21, wherein the electronic digital medium selected from the group consisting of a hard disk drive, a complementary metal-oxide semiconductor (CMOS) microchip or an electrically erasable programmable read-only memory device.

23. The system according to claim 15, wherein said data storage (b) is a software and hardware complex including a server and a database management system.

24. A unit of the automated system for verification of the consent of the party authorized to make the transaction to making the transaction by the party initiating the transaction, which includes the following:

(a) at least one device for transaction information input from the reader of the identifier of the party initiating the transaction;

(b) at least one subscriber device of an automated switched telephone network which is capable of establishing a connection with a subscriber device of the party authorized to make the transaction, of conveing the caller's subscriber address, and receive a clear-back and an answer signal,

whereas the subscriber address corresponds to the subscriber device of the party verifying the transaction, and the subscriber device of the party authorized to make the transaction can present information about the caller, and send a clear-back and an answer signal; and

(c) a control device for said at least one subscriber device connected to said at least one transaction information input device (a), including at least one database containing the identifier of the party initiating the transaction and the corresponding registered identifier of the party authorized to make the transaction, the registered identifier of the party authorized to make the transaction and the corresponding subscriber address of the party authorized to make the transaction, transaction information including the identifier of the party initiating the transaction and the corresponding transaction status,

whereas said control device for at least one subscriber device can enter into said at least one database, transaction information after the transaction information is received by said at least one transaction information input device and subsequent determination of the registered identifier of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and of the subscriber address of the party authorized to make the transaction according to the registered identifier of the party authorized to make the transaction, the said control device can call the subscriber address of the party authorized to make the transaction, and can register the transaction status after receiving a clear-back or an answer signal.

25. A unit of the automated system for verification of the consent of the party authorized to make the transaction to the making of the transaction by the party initiating the transaction, which includes the following:

(a) at least one device for transaction information input from the reader of the identifier of the party initiating the transaction;

(b) at least one subscriber device of an automated switched telephone network which can initiate a connection with the subscriber device of the party authorized to make the transaction, convey the caller's subscriber address, and receive a clear-back and an answer signal,

whereby said subscriber device of the party authorized to make the transaction can convey information about the caller, and transmit a clear-back and an answer signal;

(c) a data storage containing predetermined interconnected identifier of the party initiating the transaction, and the subscriber address of the subscriber device of the party authorized to make the transaction,

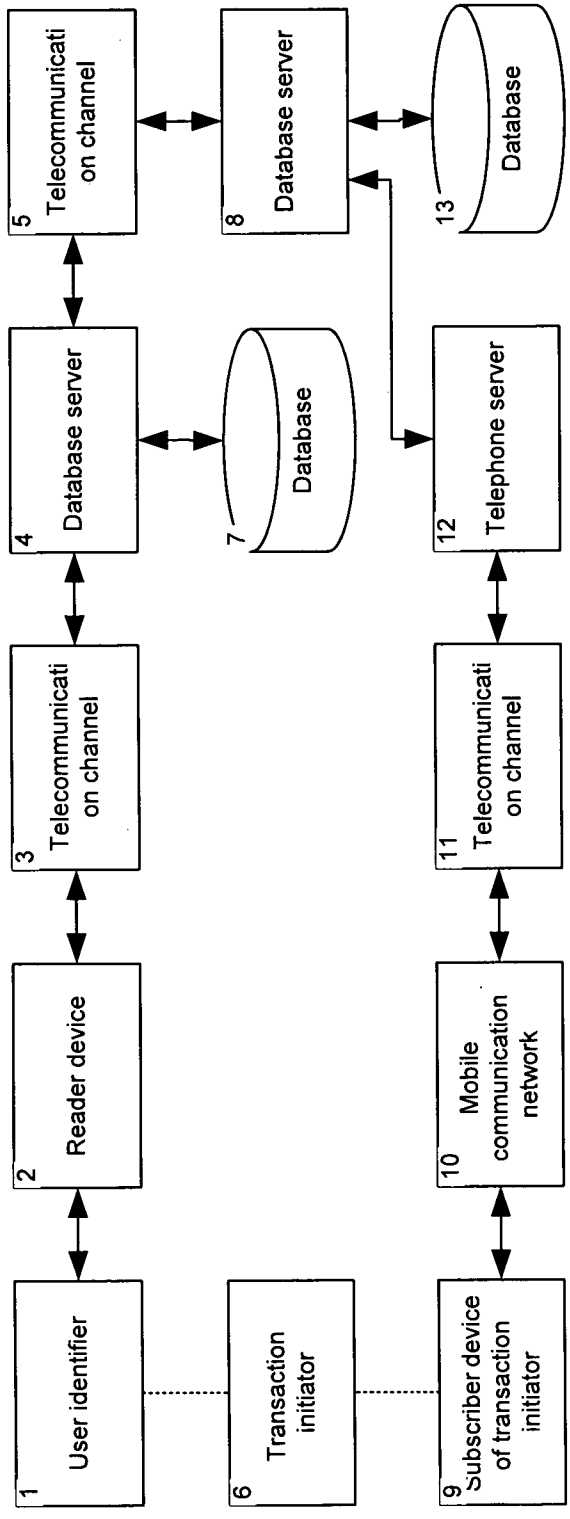
whereby said data storage can accumulate transaction information including the identifier of the party initiating the transaction, and information on transaction verification result;

(d) a data storage control device which can enter transaction information into said data storage (c) and retrieve from said data storage (c) the subscriber address of the subscriber device of the party authorized to make the transaction according to the identifier of the party initiating the transaction, and

(e) a control device for said at least one subscriber device connected to said at least one transaction information input device (a), the control device is so arranged that after receiving transaction information from said transaction information input device (a) it enters this information into said data storage (c), retrieves from said data storage (c) the subscriber address of the subscriber device of the party authorized to make the transaction, initiates a connection with the subscriber address of the party authorized to make the transaction by means of the subscriber device of an automated switched telephone network, and after receiving a clear-back signal it enters into the data storage information indicating a negative result of transaction verification, and after receiving an answer signal it enters into the data storage information indicating a positive result of transaction verification.

26. The unit according to claim 25, wherein the subscriber device of the automated switched telephone network is a GSM modem.

27. The unit according to claim 25, wherein said data storage (c) is a server containing the database, and the data storage control device is a database management system.


1 User identifier
2 Reader device
3 Telecommunicati on channel
4 Database server
5 Telecommunicati on channel
6 Transaction initiator
7 Database
8 Database server
9 Subscriber device of transaction initiator
10 Mobile communication network
11 Telecommunicati on channel
12 Telephone server
13 Database

1/9

Fig. 1

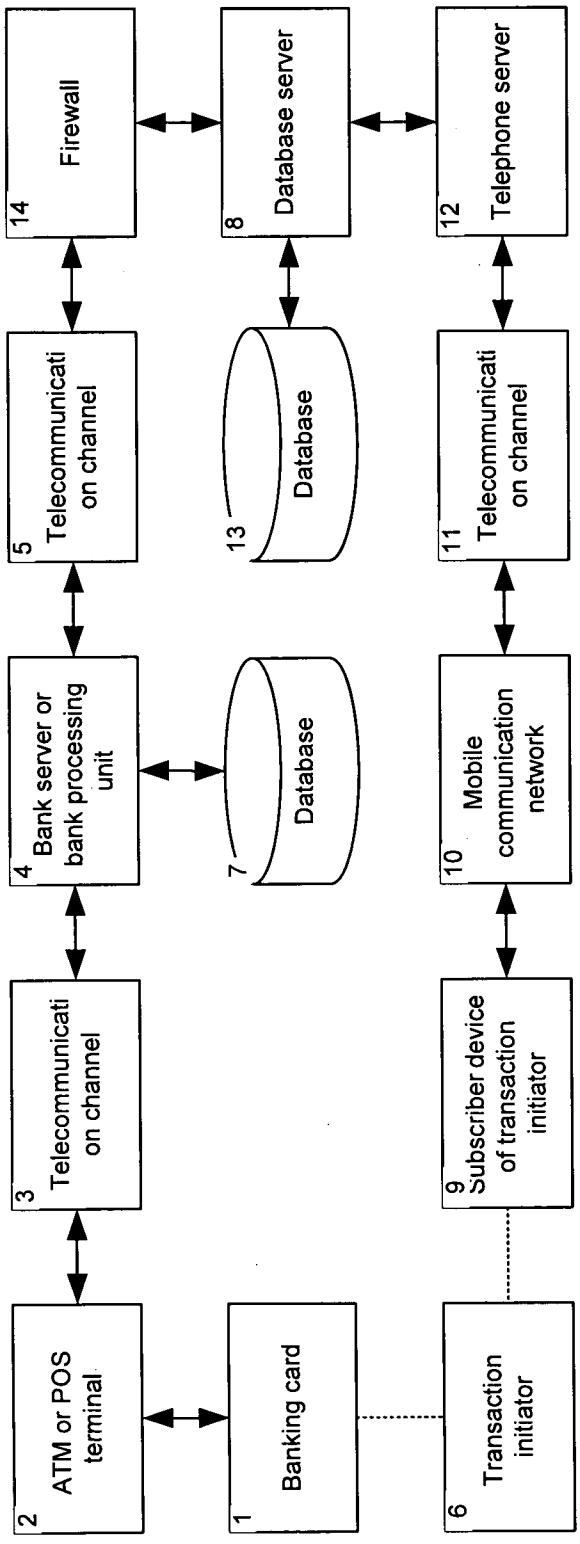

14 Firewall
8 Database server
12 Telephone server
5 Telecommunicati on channel
13 Database
11 Telecommunicati on channel
4 Bank server or bank processing unit
7 Database
10 Mobile communication network
3 Telecommunicati on channel
9 Subscriber device of transaction initiator
2 ATM or POS terminal
1 Banking card
6 Transaction initiator

Fig. 2

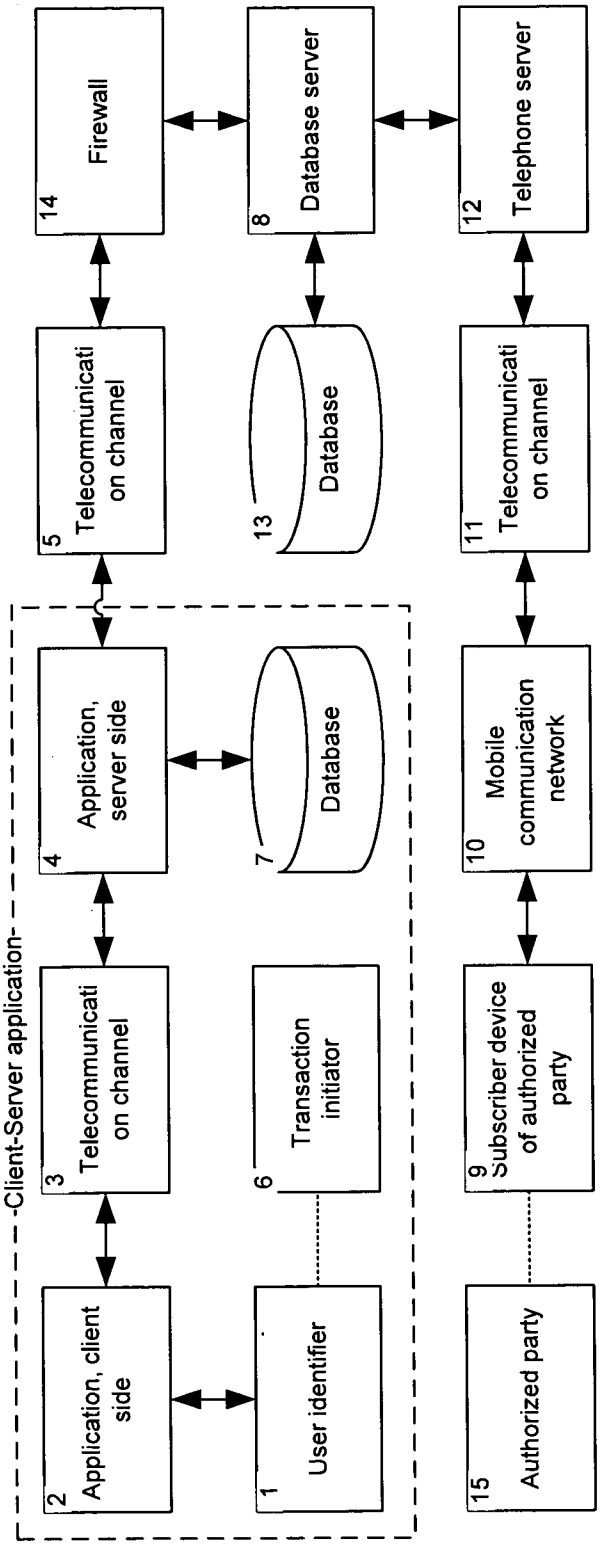

Client-Server application
1 User identifier
2 Application, client side
3 Telecommunicati on channel
4 Application, server side
5 Telecommunicati on channel
6 Transaction initiator
7 Database
8 Database server
9 Subscriber device of authorized party
10 Mobile communication network
11 Telecommunicati on channel
12 Telephone server
13 Database
14 Firewall
15 Authorized party

Fig. 3

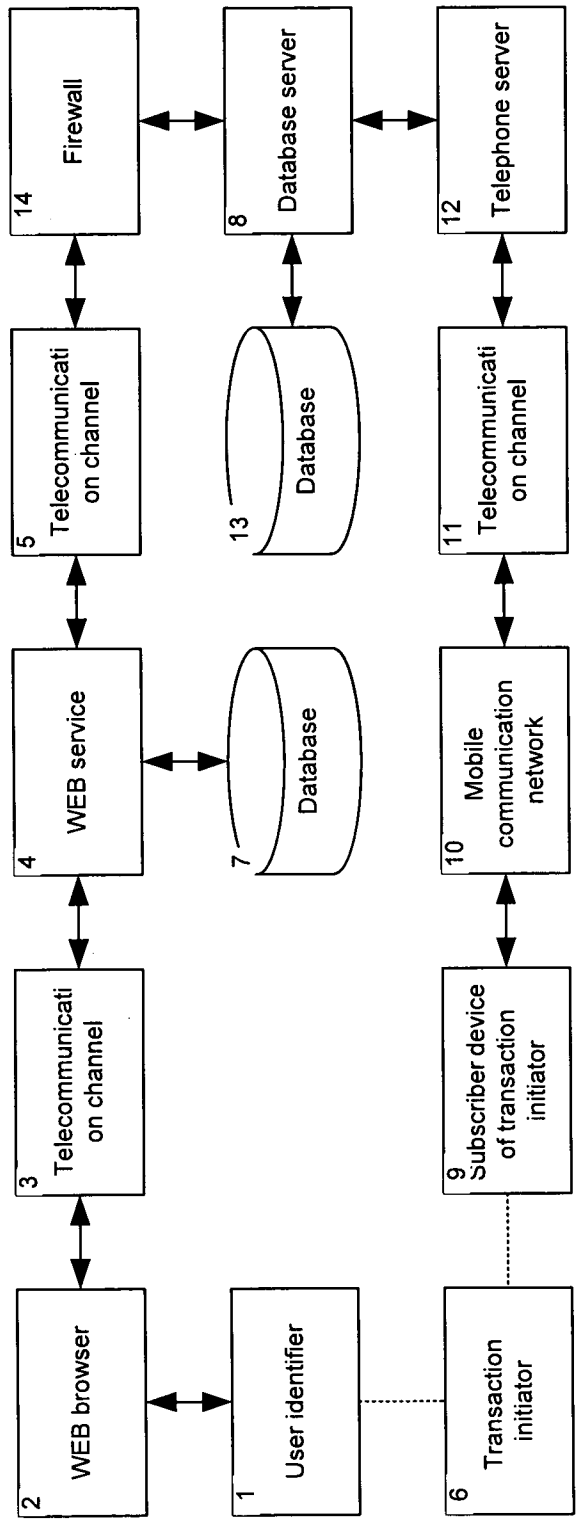
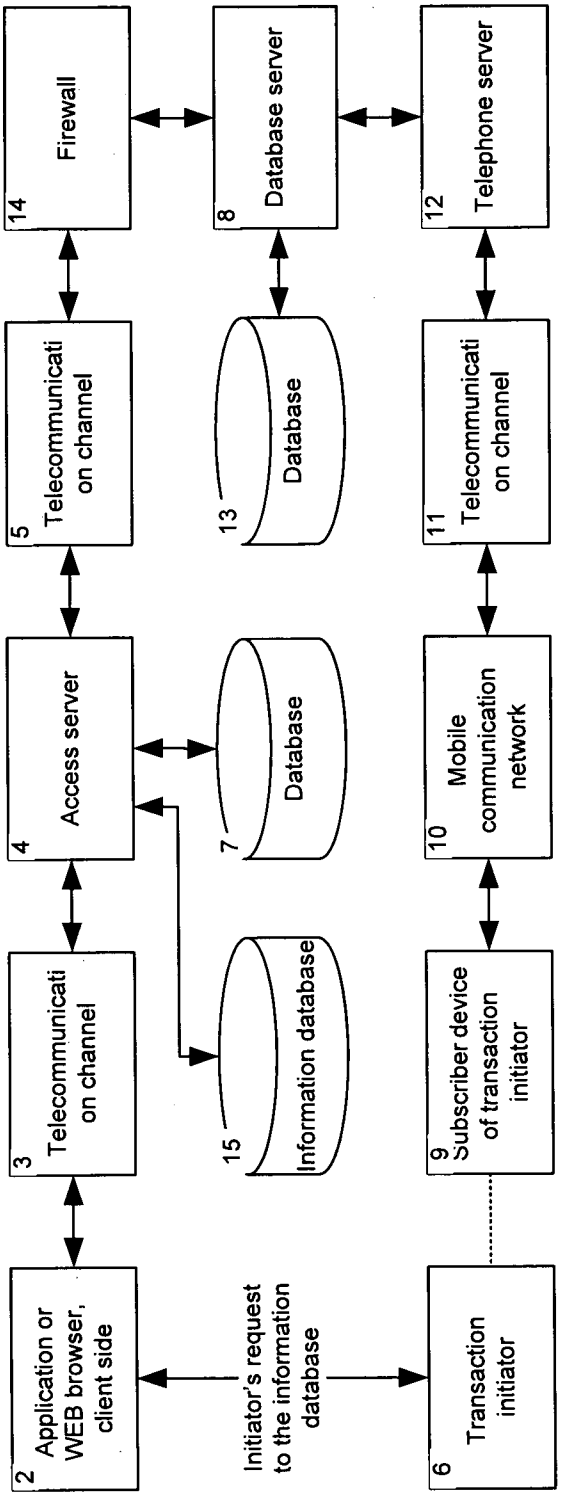

14 Firewall
8 Database server
12 Telephone server
5 Telecommunicati on channel
13 Database
11 Telecommunicati on channel
4 WEB service
7 Database
10 Mobile communication network
3 Telecommunicati on channel
9 Subscriber device of transaction initiator
2 WEB browser
1 User identifier
6 Transaction initiator

Fig. 4


2 Application or WEB browser, client side
3 Telecommunicati on channel
4 Access server
5 Telecommunicati on channel
14 Firewall
Initiator's request to the information database
6 Transaction initiator
9 Subscriber device of transaction initiator
10 Mobile communication network
11 Telecommunicati on channel
12 Telephone server
15 Information database
7 Database
13 Database
8 Database server

5/9

Fig. 5

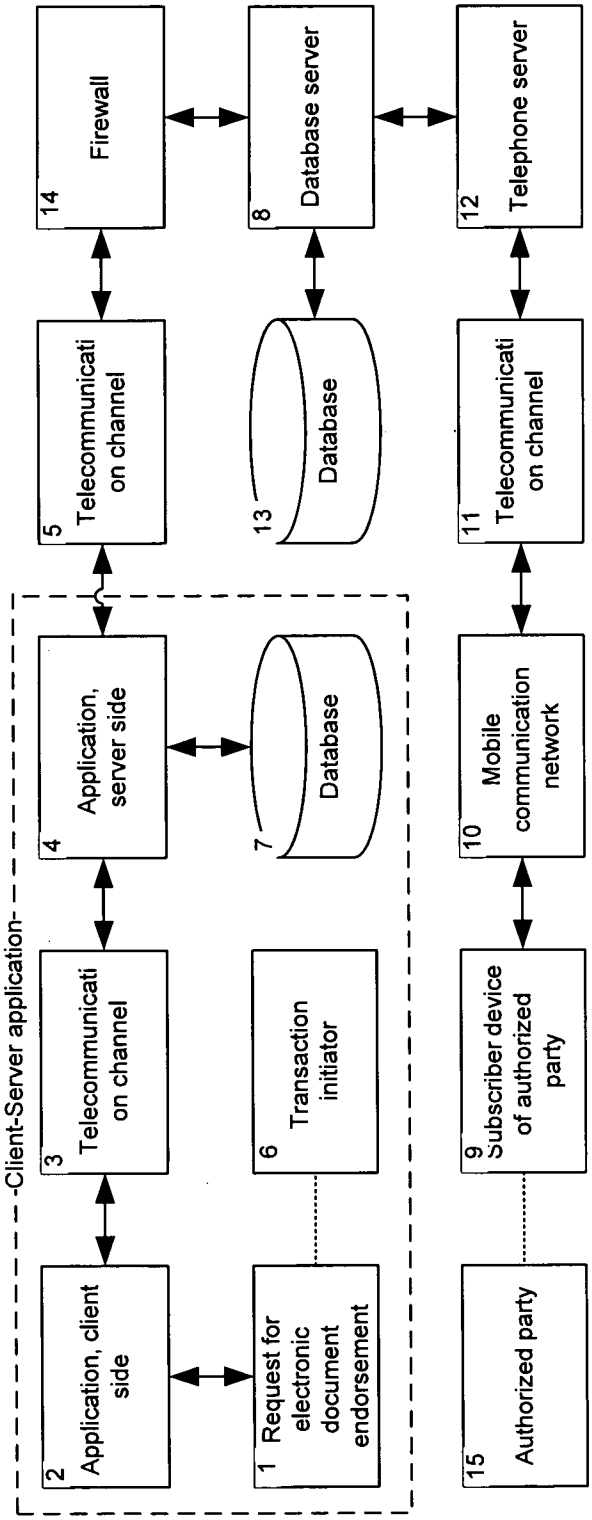

Client-Server application
1 Request for electronic document endorsement
2 Application, client side
3 Telecommunicati on channel
4 Application, server side
5 Telecommunicati on channel
6 Transaction initiator
7 Database
8 Database server
9 Subscriber device of authorized party
10 Mobile communication network
11 Telecommunicati on channel
12 Telephone server
13 Database
14 Firewall
15 Authorized party

Fig. 6

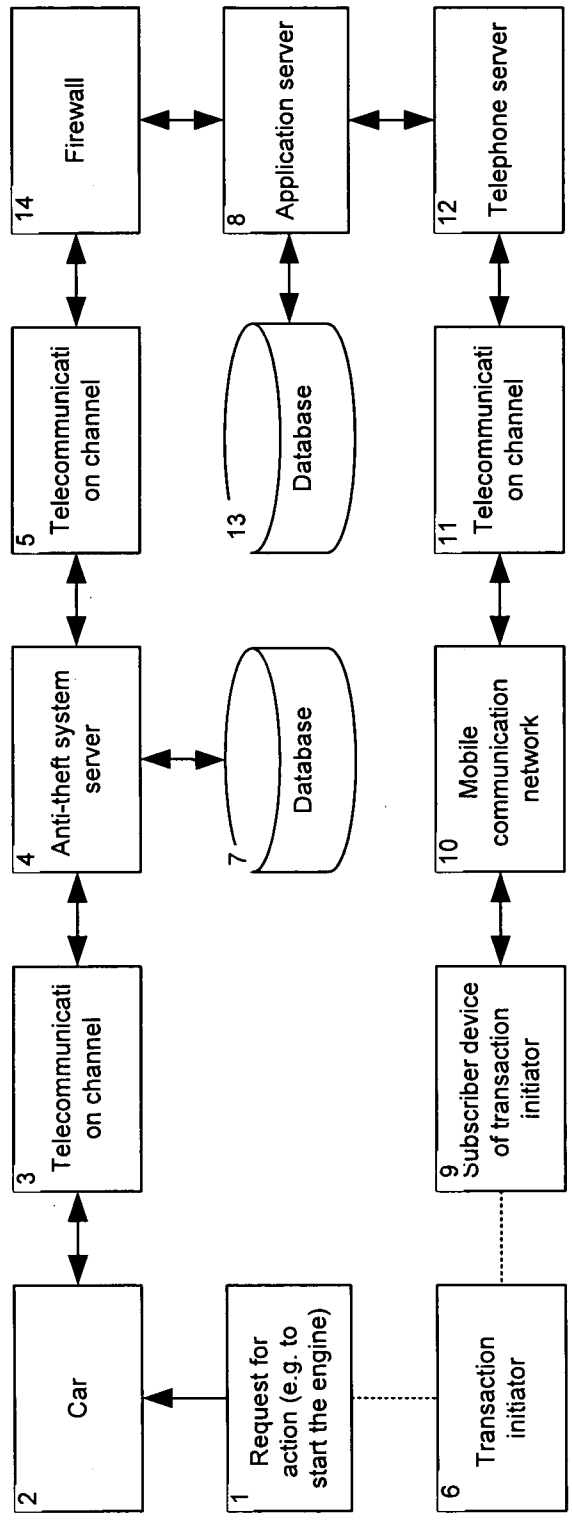

14 Firewall
8 Application server
12 Telephone server
5 Telecommunicati on channel
13 Database
11 Telecommunicati on channel
4 Anti-theft system server
7 Database
10 Mobile communication network
3 Telecommunicati on channel
9 Subscriber device of transaction initiator
2 Car
1 Request for action (e.g. to start the engine)
6 Transaction initiator

Fig. 7

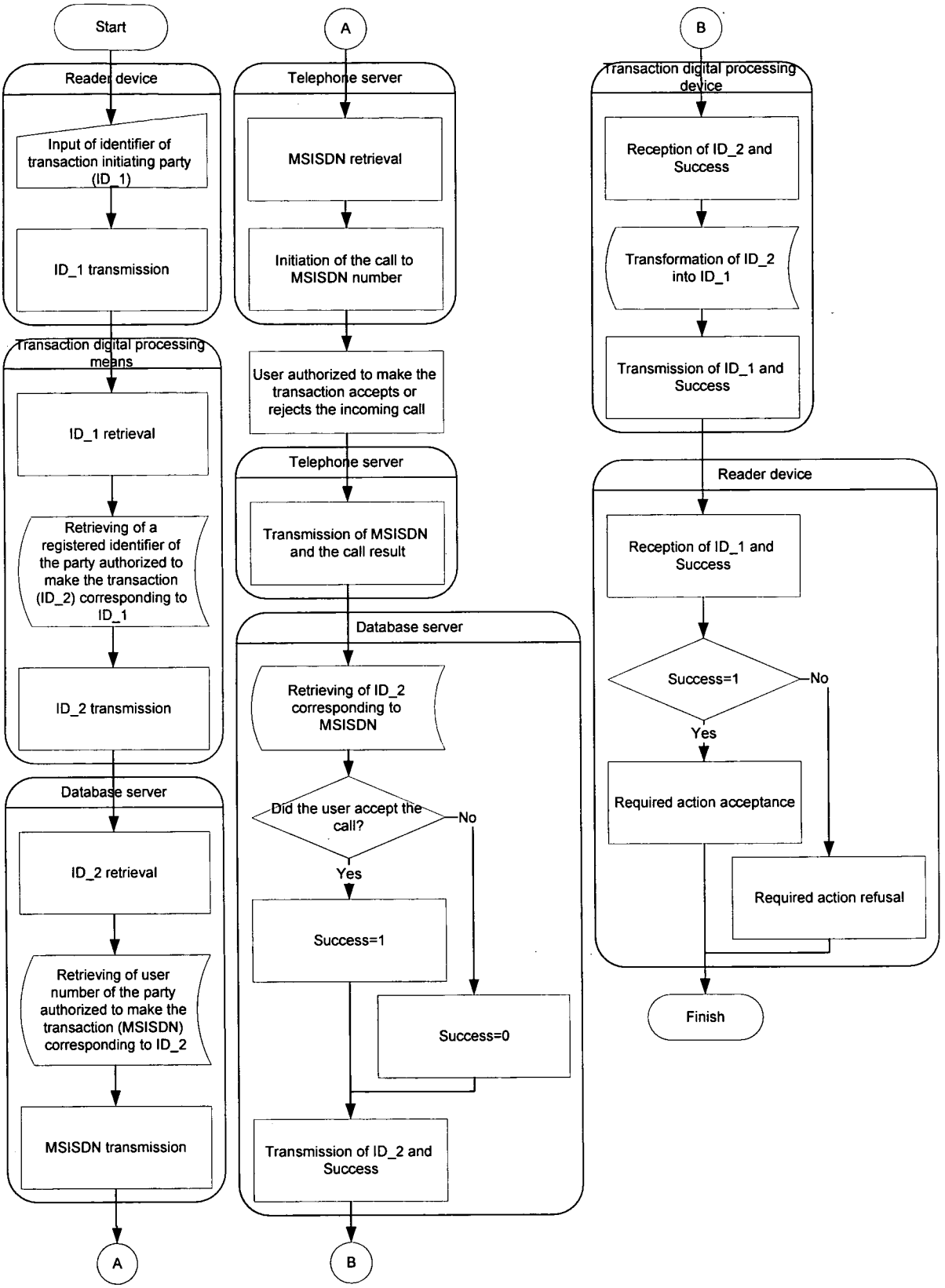

Start
Reader device
Input of identifier of transaction initiating party (ID_1)
ID_1 transmission
Transaction digital processing means
ID_1 retrieval
Retrieving of a registered identifier of the party authorized to make the transaction (ID_2) corresponding to ID_1
ID_2 transmission
Database server
ID_2 retrieval
Retrieving of user number of the party authorized to make the transaction (MSISDN) corresponding to ID_2
MSISDN transmission
A
A
Telephone server
MSISDN retrieval
Initiation of the call to MSISDN number
User authorized to make the transaction accepts or rejects the incoming call
Telephone server
Transmission of MSISDN and the call result
Database server
Retrieving of ID_2 corresponding to MSISDN
Did the user accept the call?
No
Yes
Success=1
Success=0
Transmission of ID_2 and Success
B
B
Transaction digital processing device
Reception of ID_2 and Success
Transformation of ID_2 into ID_1
Transmission of ID_1 and Success
Reader device
Reception of ID_1 and Success
Success=1
No
Yes
Required action acceptance
Required action refusal
Finish

Fig. 8

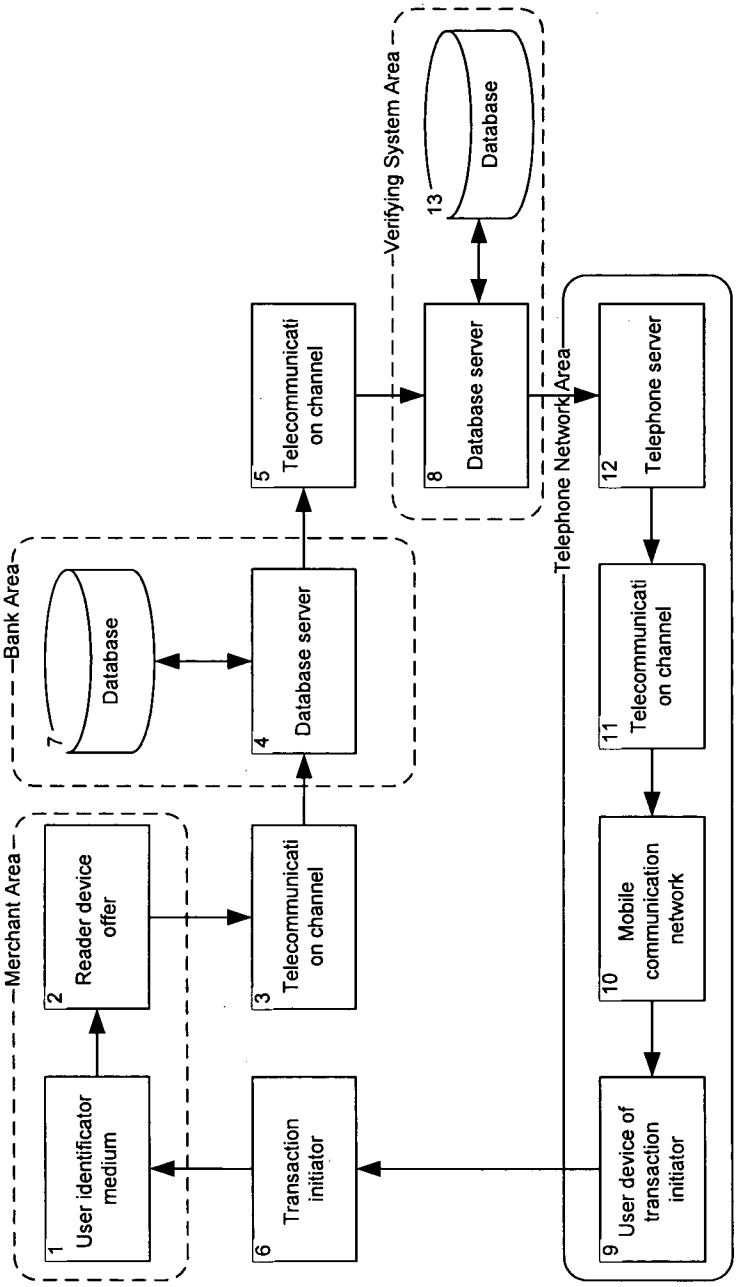

Merchant Area
1 User identificator medium
2 Reader device offer
3 Telecommunicati on channel
6 Transaction initiator
Bank Area
7 Database
4 Database server
5 Telecommunicati on channel
Verifying System Area
13 Database
8 Database server
Telephone Network Area
12 Telephone server
11 Telecommunicati on channel
10 Mobile communication network
9 User device of transaction initiator

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 2009/000582

A. CLASSIFICATION OF SUBJECT MATTER ***G06Q 20/00*** *(2006.01)*
H04W 12/06 *(2009.01)*
H04W 12/12 *(2009.01)*

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/00-30/00, H04W 12/00-12/12, H04L 12/00-29/00, G07F 7/08/ - 19/00

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

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

PAJ, Esp@cenet, DWPI, PCT online, USPTO DB, CIPO (Canada PO), SIPO DB, http://www.fips.ru

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005/045649 A1 (TELECOM ITALIA MOBILE S.P.A.) 19.05.2005	1-27
A	FR 2795897 A1 (SCHLUMBERGER SYSTEMES) 05.01.2001	1-27
A	RU 2296367 C2 (GIZEKE UND DEVRIENT GMBH) 27.03.2007	1-27
A	RU 2301449 C2 (ZAKRYTOE AKTSIONERNOE OBSCHESTVO "INTERVEIL") 20.06.2007	1-27

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

* Special categories of cited documents:
"A" document defining the general state of the art which is nit considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 2010 (28.01.2010)	04 March 2010 (04.03.2010)

Name and mailing address of the ISA/RU FIPS
Russia, 123995, Moscow, G-59, GSP-5,
Berezhkovskaya nab., 30-1
Facsimile No. 243-3337

Authorized officer

G. Smirnova

Telephone No. (499) 240-2591