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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 January 2017 (12.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/006194 A1

(51) **International Patent Classification**:
G06Q 20/08 (2012.01) *G06Q 20/36* (2012.01)
G06Q 20/32 (2012.01) *G06Q 30/06* (2012.01)

(21) **International Application Number**:
PCT/IB2016/052857

(22) **International Filing Date**:
17 May 2016 (17.05.2016)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
P22201504072 7 July 2015 (07.07.2015) ID
P22201504073 7 July 2015 (07.07.2015) ID

(71) **Applicant**: **DOWNER, Albert** [ID/ID]; Jl Tentara Pelajar GG. 7A/3, 003/004, Kandangpanjang, Pekalongan Utara, Pekalongan (ID).

(72) **Inventors**: **PRABOWO, Hanung**; Mlese RT 002 RW 001 Mlese Cawas, Klaten (ID). **FEBRIANTO, Luky**; Dusun Pekandangan Widodaren RT 048 RW 007 Desa Widodaren, Petarukan., Pemalang (ID). **FEBRIYANTORO, Fajar Indra**; Klampok RT 002 RW 013 Kelurahan Klampok, Purworejo Klampok, Banjarnegara (ID). **LEE BALADA, Sallith**; Dusun Karang Wetan RT 001 RW 001 Pucang Secang, Magelang (ID). **AINUL YAQIN, R. Ahmad**; Dusun Kebunlaut RT 001 RW 003 Sawahmulya Sangkapura, Gresik (ID). **FIRDAUS, M. Arif**; Kp Baru RT 005 RW 009 Cakung Barat, Cakung Jakarta Timur, Jakarta (ID).

(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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) **Title**: SYSTEM OF PAYMENT MADE IN REAL TIME

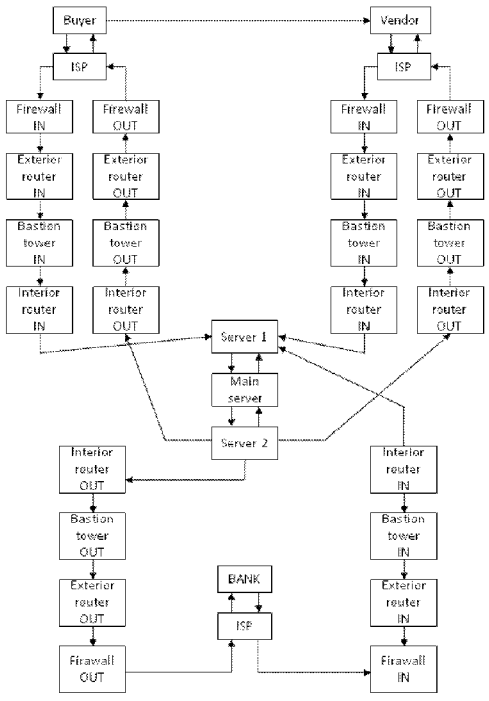


FIG. 23

(57) **Abstract**: SSP is a complete system of financial transactions and wallet management system, transactions being made in real time from any mobile device without contact, without credit or debit card, and without any transfer of sensitive data between parties in a transaction. Connections without contact between the parties in a transaction are made via NFC, QR code or SIM card. During such connection, only data which are not sensitive are communicated. Data transmissions between users and the server are encrypted and transported via a one-way road, following an asymmetrical system and along parallel paths, without any possibility of going back. The application which is downloaded on the mobile device is only an interface that contains no sensitive data and the virtual keyboard application prevents any capture of data by the mobile device.

WO 2017/006194 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

— *with amended claims (Art. 19(1))*

DESCRIPTION

System of payment made in real time

ONE-WAY PAYMENT METHOD WITHOUT THE TRANSMISSION OF SENSITIVE DATA USING THE TECHNIQUE OF ASYMETRICAL AND PARALLEL PATHS.

TECHNICAL FIELD OF THE INVENTION

This invention is an application of scientific studies in the fields of data security, financial systems and applications and, particularly, in financial information systems.

It is a secure payment system without the need for contact or the use of any bank card or credit card. Payment can be generated from any mobile device, connected or not connected, towards any fixed or mobile device, online or offline. The system uses for all transactions a special device that we have created.

Securing data is a way to protect data against all threats, anytime and anywhere. The data security is not merely just about protecting data at rest, but also about securing each data flow when it is conveyed within an IT network.

PREVIOUS TECHNIQUE

Not so long ago, when someone wanted to make a financial transaction, they had to go to a bank. If relations with the bank were good, the order could be given by e-mail or phone. In which case, it was still necessary to go to the agency to sign the transfer slip to regularize the situation.

Technique in use nowadays

In a traditional transaction process performed from a mobile device, the modus operandi is as follows:

First, one has to download the application on his Smartphone or tablet.

Then, he has to use the keyboard of the Smartphone or tablet to register, that is to say, create a password, provide personal and banking data (register his bank

card or credit card) and, in some cases, wait for a confirmation email to validate the registration.

All this data generally remains in the Smartphone or tablet and in secure servers.

When you want to perform a transaction, you have to open the application downloaded beforehand, enter your username and password and enter a set of data necessary to accomplish the transaction.

Either you have to re-enter your bank details or, as in most cases, your bank data is recorded directly on your Smartphone or tablet, or in the company server that manages the transactions.

In these systems, in order for the transaction to be successful, the banking data of users and their personal data are transferred from the buyer to the seller, which retains at least a trace of them, and then are transmitted to the banking organization.

The transaction cannot take place before the full circuit has been completed. The transaction will be approved if all the data match. But the displacement of the money, for the user to be credited, will be shifted in time. At best a few hours, at worst several days (up to 12 days for PayPal).

By using the remote payment system PayPal or PayPal One Touch, the connection information is stored in the device. One Touch keeps you always connected and you can pay without entering a username and password. The money transfer is done by means of a card or from a bank account and is not in real time. PayPal uses the email address and password as login detail. The sensitive data (banking, personal) are stored in the Smartphone or tablet.

Google wallet is an application for Android only, which allows a payment with NFC technology. The wallet is linked to one or more credit cards. All the data is in the Smartphone. The transaction is subject to the credit card system and is not carried out in real time.

It is essential to have a credit card in order to use Apple Pay. It is either already saved in your iTunes account or you have to encode it into your device by taking a picture of it. Afterwards, your bank verifies your card details and

authorizes or not its use with Apple Pay. The user can use this system only on a terminal that accepts it or to purchase online at the condition that the site also accepts that same system. There are several limitations, for example, the bank must be a partner because it should allow or disallow the use of the card and the merchant must have an appropriate terminal. The payment is subject to the rules of bank card transactions. Therefore, the payment cannot be in real time.

With Apple Pay there is no bank data transfer when making a payment. Only a reference number attached to the card in use, which is stored in a chip on the device, is transmitted. The data is encrypted, but current events have shown us the limits of the cryptography. A security code specific to the transaction is used to process the payment when a purchase is made. In addition, each payment requires a Touch ID (fingerprint reading) or a password. The seller has no knowledge of the customer's bank details or identity.

Hence, Apple Pay is only another intermediary in the transaction chain that is only found on the App Store.

Subsequently, the transaction follows its traditional path between the banks.

Every payment made by card is done in two steps. The first one, by far the most vulnerable, is that of the authorization, because it involves the transmission of sensitive data. The second one is the one of settlement.

During the authorization phase, it is necessary to check the credit card and the sensitive data it contains. In the case of a debit card, it is also necessary to determine whether there is sufficient money in the account for the payment to be done.

The authorization phase starts with the reading of the card by the payment application and analysis of the data it contains. This is done at the internal infrastructure of the seller, which records the information on the card and sends it to the gateway or adequate processor.

The gateway and processor retain the transaction details and send them to the "acquirer" (the bank which authorizes the payment of the transaction and determines the amount of commission that the seller has to pay) that transmits via the "Payment Brand" (the credit cards or third parties delegated by them) to the "issuer" (the customer's bank which holds his account and issues the card),

in other words, someone who keeps all the data related to the cards and their holders and checks their banking situation in real time.

If the conditions for the payment to be made are met, then the “issuer” returns an approval response to the “acquirer” who transfers it to the POS, which firstly red the information stored in the card.

Then follows the settlement phase, following the same path, but this time without transmitting any sensitive data.

The acquirer will then credit the merchant’s account, while the issuer will send the invoice to the card holder.

However, in practice, given the great complexity of the payment process, the proliferation of card types and payment methods, the intervention of a “man-in-the-middle” is virtually systematic. They participate in the analysis of sensitive data and its transport to the competent acquirer.

The basis of the banking system is interbanking. This allows the credit card to be accepted regardless of the name of the merchant’s bank and the one of the client.

A system is called “four corners”, when it connects four actors: the cardholder, the merchant, the cardholder’s bank (called the “issuer” because it issues the cards) and the merchant’s bank (called the “acquirer” because it acquires the transactions). “Four corners” systems example: CB, MasterCard, Visa.

A system is called “three corners”, when it connects three actors: the cardholder, the merchant and the system that provides by itself both the card issuing function and transaction acquisition function. The role of the banks in the “three corners” system is to distribute and market the products and services of the system. “Three corners” systems examples: Amex, Diners, charge cards...

In this card payment system, the user (the seller) is not credited in real time. It undergoes clearinghouses.

The clearinghouse is a financial institution, whose mission is to limit counterparty risks in derivatives markets. The clearinghouse monitors positions and is the sole counterparty for all operators. This means that it is the buyer to

all sellers and the seller to every buyer. The clearinghouse is made up of the clearing members, who are guarantors of the performance of the operation. Major European clearing houses include among others LCH Clearnet and Eurex Clearing.

In order to avoid these problems (the lack of security and the lack of speed in transactions), we offer a system that is transparent, easy to use and fast, because operating in real time and totally secure.

It is in this context and bearing in mind the needs of the users and the necessary conditions of security that any electronic payment system must meet, especially when it is generated from a mobile device, that we propose a system called “Secure System of Payment” or abbreviated SSP, that comes in SSPcl for payments from a Smartphone, SSPsc for payments made from a non-connected phone using SIM card and in SSPqp for ultrafast small payments, and their equivalents in fix terminals POS1, POS1.2, POS2, POS2.1 or POS2.2.

DISCLOSURE OF THE INVENTION

I. Failures of current mobile payment systems

Electronic means are daily used in the context of financial transactions from individuals to individuals or for commercial purposes. The problems faced by such operations are related to their transparency, speed of execution, ease of use and especially their safety.

It is common knowledge that the Internet and in general, everything that is connected is likely to be attacked and the conveyed or stored data is an easy prey.

It is also common knowledge that Smartphone are absolutely not reliable. Likewise, the payment cards or credit cards are not reliable, because they carry sensitive information.

In addition, transactions are not made in real time and traders sometimes have to wait up to twelve days to be credited and to use the money that belongs to them.

The flaws of the existing systems are related to the problem of security (or lack thereof) in both the mobile device itself and during the transfer of data, and to the speed with which the recipient receives its due.

- *Regarding the safety*

The first flaw lies in the use of a connected mobile device, be it a Smartphone, a tablet or other, to complete a transaction.

Indeed, every time a Smartphone or tablet is used to record data in an application, as safe as it may be, we use the keypad on the device or sometimes the photographic function. All data stored in the mobile device or even those which are only transiting through the keyboard are found on the device's memory.

As the Smartphone is never completely secure, it implies that the data contained by or transiting through it are vulnerable to all external attacks, even if encrypted.

A second flaw lies in the transfer of sensitive data (banking and personal data). During a transaction, banking and personal data are transmitted between stakeholders (user/server/financial institution/clearing house). It is possible to encrypt data but it is also possible to intercept and decrypt them.

- *Regarding the speed of settlement of the transaction*

A final major drawback is time frame. None of the existing systems enable money transfers in real time, leading to problems for small traders who do not always have working capital available.

II. Solutions provided by the innovation

The solution provided by our invention at first is the design of the data-management and storage system on our servers and of their transmission from or to any fixed or mobile device, knowing that such device will not receive any sensitive data and no sensitive data is conveyed or communicated to the parties or between the parties to a financial transaction when it is processed.

A. Regarding the safety

i. Safety when transporting data:

Transactions take place between parties using one of the following means for direct payments or via Internet:

1. NFC
2. QR code
3. SMS for connected phones and for those which are not (SIM card).

And for remote payments:

1. Transfer to other users with SSP account
2. Bank transfer to a SSP or non SSP account of a user or a non-user that is held or not in a bank extraneous to the SSP system.

Under no circumstances does the system use any bank or credit cards.

The flow of data necessary to any financial transaction is conveyed through a one-way system of transmission using the technology of paths that are asymmetrical and parallel. Each party is only in contact with the server during the transaction. In case of a connected mobile device used to initiate the transaction, the parties to this transaction are communicating to each other only one code generated by the server. In the case of a non-connected mobile device, there is no communication between this device and the other party to the transaction, as the server is sending the code directly and separately to each party.

This code is the identifier of the transaction. It is kept by the server and is part of the history of transactions. It is kept in the archives because it identifies the transaction and its stakeholders.

There is no connection between the users and the banks in order to prevent sensitive data being lost at either end during the process of financial transactions.

The only connections that exist are those between the users and the server and, on the other hand, between the server and the banks.

ii. Security of data at rest

Figure 23 shows the circuit that the encrypted data have to follow to reach the server and vice-versa following the technology of asymmetric and parallel paths.

The security of the main server is provided not only by its special environment but also by the absence of contact between the main server and the Internet.

The information, whether sensitive or not, go through a series of filters, each having a specific mission to prevent the violation of the one-way routing channel and detect intrusion or corruption attempts. They are received by a "SERVER IN", a server that is the culmination of transportation point to the "outside world" and the boundary between the "outside world" and the one of the server with which it communicates via a private channel off external connection.

The communications from the main server are sent via another channel, the "SERVER OUT", which sends them to the recipient through a series of filters, different from those used for the input path, but with the same functions.

iii. Security in mobile devices

Still totally secure as there is no sensitive data in the mobile device used to perform a transaction. Not even the application itself as it is in the main server.

What is installed in the connected mobile device is only an interface.

The interface generates a virtual keyboard, which eliminates the need for use of a physical keyboard from the mobile device. That is to say that what is used to send information is not the keypad of the mobile device, but the one that was created for the program and that is part of the SSP interface.

The use of the virtual keyboard with automatic, immediate and encrypted shipping of any digit to the main server, without having to cause it, prevents the existence of any trace in the cache memory of the mobile device.

iv. Risks mitigation

Since the system of payments by SMS from or to a non-connected mobile device (SSPsc: Secure System of Payment sim card) is less safe than the one set up for transactions via the Internet (from the point of view of authentication

and validation) and because the fast payment system (SSPqp: Secure System of Payment quick pay) prevents, given the speed with which it is to occur, the performance of the whole security procedure established by SSP, a sub-wallet has been created next to the wallet.

This sub-wallet can only contain a limited amount and only allows a certain number of transactions per day with a maximum cap per day and per transaction, all of which can be predetermined by the user.

However, default limits are established.

The payment made through a mobile device connected (SSPcl: Secure System of contactless payment) is initiated from the user's wallet. The payment that is made by a non-connected mobile device (SSPsc) or by a connected mobile device, but to a quick payment POS (see below) (SSPqp and POS2.1) is initiated from the user's sub-wallet.

Each user of SSPcl can have a wallet and a sub-wallet, but each user of SSPsc can only have a sub-wallet.

In addition, as the data is transferred via SMS (see below), the user of a mobile device which is not connected has only one identification code (3 letters and 3 numbers).

B. With regard to the speed of transfer

In general, what is said for the wallets applies to the sub-wallets.

With the SSP wallet and thus sub-wallet management system, the financial transaction is finalized in the moment in which it is made.

How it works:

- The SSP general wallet contains user's wallet and all the bank accounts in which its money and users' wallets are - regardless of the country in which they are located - and the related money which is in the banks in which SSP has an account (Figure 1 shows the Wallets organization in SSP account in a bank).
- SSP has an account in a set of banks. Each account contains money from the users which are clients of the bank in which the account is

opened and the money of SSP and/or the money of the client-users who do not have bank accounts, but who chose to have their wallet in a bank that houses a SSP account. Each SSP account contains as many wallets as the number of SSP clients related to this bank, plus the SSP wallet itself.

- Each SSP client who holds an account in a bank, in which SSP has also an account, will have his wallet placed in this bank without moving. SSP clients who have no bank account can choose which bank their wallet will be placed in. By default, SSP will place their wallet in the bank of his choice.

Each time a payment is made by a user, the amount of that payment is transferred from the wallet of the user to the wallet which SSP has in the same account in the same bank.

Meanwhile, in the bank of the recipient, the SSP wallet is debited by the same amount while the recipient's wallet is credited. Whilst the operation is done within the same account, it is only a set of accounting entries. (Figure 2 shows what happens when a transaction that involves two banks is on process and Figure 3 shows what happens when a transaction within one bank is on process).

When the transaction is validated by each party, the transfer takes place and each party receives the message of the result in the application. The money is in that moment already available.

III. The benefits of the innovation

The financial system in question is a system that efficiently manages and regulates, on the one hand, the transfer of funds from one person or group A - having an electronic wallet managed by SSP - to a person B or a group B without regard to whether the recipient has a SSP wallet or not. On the other hand, the system manages and regulates the accounting of funds that each user has in his electronic wallet and, finally, it also provides financial facilities, among which the payment system necessary to fund commercial activities.

The benefits that this invention provides for transactions generated from a mobile device are as follows:

- Ease of use and rapidity in handling and in result (in real time) and effectiveness of the transaction itself between the users, whether they are close or not.
- Ease of long-distance payments for SSP users (see below).
- Financial inclusion of the smaller players as they can use their non-connected phone for all financial operations just like a connected mobile device would allow them to and they can have a wallet without having to own a bank account (see below).
- Total security ensured not only by the triple authentication system and the validation one, but especially thanks to the asymmetric, unidirectional and parallel routing of encrypted information.
- As far as the security of transactions is concerned, our payment system operated from a virtual keyboard on the mobile device - that is by definition insecure (Smartphone, tablet or simple non-connected phone) - does not use any transmission of confidential and sensitive information between the parties to the transaction.
- Moreover, even the transmission of non-sensitive data is protected by a cryptographic system that we have designed and by the environment that protects the main server of any attempted intrusion or corruption.
- The data itself are protected when not in use, as well as is the management of user accounts as they are managed and stored without any contact with the outside world.
- As far as comfort during use and speed with which transactions are made are concerned, the use of NFC, QR code or Bluetooth enable us to safely send the non-confidential information from a mobile device to another or to a fixed terminal that we have created.

The SSP payment system allows shopping in stores through terminals (Point of Sale: POS), which we have created.

- **POS 1:**

- POS 1 is a double faced terminal, completely independent, that thanks to its modem is directly connected to the server with which it communicates

in the same way as the connected mobile devices, and includes a keyboard (used to select the type of transaction and record the amount owed) and two screens, a buzzer, indicator lamps of the success or failure of the transaction, as well as the functionalities of contactless NFC, QR code and SIM card.

- As it is not equipped with a camera, it is the mobile device of the customer that reads the QR code generated by the server on the POS1 screen.
- It is the only POS (outside of a mobile device that is used as POS), which accepts the payment initiated by a non-connected mobile device. The seller has the option to choose the type of media to initiate the payment.

- **POS2:**

- POS2 is a single-face terminal that includes a buzzer, indicator lamps of the success or failure of the transaction, a camera and an Ethernet port as well as the functionalities of contactless NFC, QR code.
- It is the POS2 that reads the QR code containing the identifier of the transaction generated by the server and displayed on the mobile device of the customer.

- **POS 2.1:**

- Also called POS qp for quick payments (parking, train, bus, etc.), which is a single-face terminal that includes a buzzer, indicator lamps of the success or failure of the transaction and an Ethernet port as well as functionalities of contactless NFC.

- **POS 2.2:**

- POS 2.2 is a single-faced terminal, consisting of two removable parts, including one mobile part that includes a buzzer, indicator lamps of the success or failure of the transaction, a camera and the functionalities of contactless NFC, QR code and a second part with an Ethernet port, Bluetooth and printer.

- The terminal reads the QR code containing the identifier of the transaction generated by the server and displayed on the mobile device of the customer.
- The printer provides instant print of the transaction data supplied to it by the mobile part of the server that uses Bluetooth to do this.

On the other hand, our wallets management system ensures the transfer of funds in real time: the merchant or recipient is credited in the second and can immediately use his money either by paying an invoice to a third party account, or by transferring his money to one of his accounts or by withdrawing the money from a cash machine (ATM) which accepts the SSP system, without having to wait as it is the case with other payment systems.

This is an innovation in the back-end of the infrastructure of payments and in the field of financial inclusion of small players (SSPsc).

SSP is thus a totally secure contactless payment system that uses the techniques of asymmetric and parallel path without debit card or credit card, from a mobile device, connected or not connected, and a management system of electronic wallet that each user opens by registering and that is credited or debited in real time with instant notification, depending on the type of transaction.

The system uses 3 programming languages: Python for the server and administrator, Java for Android or iOS user for the mobile device. The site itself was created by using the PHP programming language.

IV. How it works

A. Registration

1. For SSPcl (contactless)

The registration is done in two steps:

Figure 4 shows the registration proceeding.

The first step is downloading the application from the SSP website, from Play store or from App store.

What is downloaded by the user is only a temporary application.

The application is automatically installed by itself. Then the user has to agree with the terms of use.

The second step: after notifying his agreement, the user will download the main application from SSP Server. He has to install it and open it.

What is installed on the connected device is an interface that allows the user to be in touch with the Application itself that is stored in the main server.

The user must proceed to his registration.

He has to choose between SIGN UP (for new user) and MIGRATION (when the user has already an account). He has to indicate his full name, his e-mail address and his phone number and verify the accuracy of his details.

What is communicated to the server, it is only the name, the e-mail address and phone number that have been entered together with the IMEI (number used to uniquely identify a mobile device) of the mobile device that is used.

The server automatically generates a code of 3 letters that is sent by SMS to the specified telephone number. User has to reproduce these 3 letters.

This is to verify that there is no discrepancy between the provided information and reality.

The user will then create an authentication code that must consist of three letters and three numbers and a validation code for the transactions, made of 3 letters.

At this stage the user can leave the registration proceeding or continue it by answering some questions.

When the user enters personal data from a connected mobile device, he does this by using the virtual keyboard of the system (and not the one of the mobile device) so nothing is transiting through mobile device. This is true not only for the registration process, but also throughout the use of the application.

2. *For SSPsc (not connected phones)*

The user of a non-connected phone has the choice to register either via the website https://s6pay.com or by using the system SMS.

- Website

The user can register on SSPsc via s6pay.com. The user can click the “client registration” in the website.

The user utilizes the virtual keyboard that appears on the page of the website to fill in his phone number, email and password.

Then, the user has to click the “register” button.

- SMS

If the user has no internet access, then the user can register via SMS.

The user has to send a SMS to the phone number of SSPsc SMS server, with the keyword ‘REG’ following a slash (‘/’) and his chosen password (six digit, the 3 first digits are letters and the last 3 digits are numbers).

The user will then receive a complete registration notification via SMS.

3. *For the professional*

The professional (one who uses SSP as means of payment in connection with his professional activity) must register via the https://s6pay.com website using the virtual keyboard on the site, so that the characters typed are transferred to the server without them passing through the website.

4. *Data transfer*

The application never uses the keypad of the mobile device but its own virtual keyboard.

For safety, all data conveyed from the mobile device to the server or vice versa is encrypted and transferred using the technique of one-way asymmetric path with impossibility to go back by the same route.

Asymmetric way means that the path used to send information from a fixed or mobile device is not the one by which information communicated from the server will return to it : This is a one-way transfer of information and the server that receives the information is not the one which issues them.

The cryptography that is used is also **asymmetric** in the sense that the key used to encode the message (public key) is not the same as the one used to decrypt it (private key).

B. The payment mechanism

The contacts are made between the customer (or ordering party) and the server on the one hand and between the merchant (or beneficiary) and the server on the other hand: it is a system that works in unidirectional and parallel tracks.

The authentication is done by the user who inserts his identification code of 3 letters and 3 numbers.

The server then compares the password to the phone number and the IMEI of the mobile device.

After being authenticated to the server, each party to the transaction communicates to the server the amount payable or receivable, which must be the same for each of the parties otherwise the transaction is denied.

This information is routed to the server with two unidirectional and parallel channels, one for the ordering party and one for the beneficiary.

The server then communicates to the party that initiated the operation, via another starting point and using another way, the registration number it has assigned to the transaction and which will remain always attached to it.

It is through NFC, QR code or via SMS technology that the transaction number will be communicated to the other party. This is the only contact between the parties to a transaction.

This transaction number will be immediately routed to the server through another one-way path without the recipient making any adjustment.

If the server receives back the transaction number, it will separately ask each party to validate it. Each party will then insert the validation code.

Once validated, the transaction is effective. Otherwise, the transaction is cancelled, but the server holds the number it has assigned to it.

Afterwards, the application will let each party know the result of the transaction.

The transaction will only be effective if the amounts communicated separately to the server by each party match each and if the transaction number sent by the server to a party to the transaction is returned to him from the other party and if the validation codes are valid.

The originality of the system lies in the fact that:

- There is a triple degree of identification control, namely the telephone number and the IMEI, which are controlled automatically by the server and the ID that the user must have inserted.
- There is a triple validation system, i.e. the correspondence between the amounts reported separately, the return of the number of the transaction by the second party to the transaction and the validity of the validation codes.
- Each party only communicates with the server separately and the only connection between them, when it is required, is only to transmit the number that the server has assigned to the transaction.
- The contact system between users and the server is that of an asymmetric and parallel path.

The process:

- <u>When the payment is generated from a connected mobile device:</u>
  - **In direct payment mode**
    - *Towards POS1*

Figure 5 shows the transaction in direct payment mode between Smartphone and POS 1 with NFC.

1. The merchant indicates on the POS1 the amount payable by the purchaser, which appears on POS1 screen.
2. The POS1 automatically announces to the server the transaction to be made.
3. The server sends to the POS1 the reference number he has attributed to the transaction.

4. This reference number is either displayed on POS1 in QR code format (Figure 6) or via NFC (Figure 5).
5. The client enters in the application the amount to be paid.
6. The client receives the reference number from POS1 either by NFC contactless transfer (Figure 5) or by scanning QR code on POS1 screen (Figure 6).
7. In turn, the client communicates to the server the amount entered in the application and the reference number.
8. The server checks the amount and the reference number and if they match, the server will ask the client to validate the transaction. Otherwise, the transaction is cancelled.
9. The client sends the 3 letters validation code. The transaction is terminated if the code is valid. Otherwise, the transaction is cancelled.
10. The server sends the result of the transaction to each party and the status of their account after the transaction.

- *Towards POS2 (qp): with fix amount only*

Figure 7 shows the transaction in quick payment mode between Smartphone and POS 2 with NFC.

1. The client (payer) chooses in the application the “quick pay method” and he chooses NFC.
2. The application automatically sends a transaction request to the server.
3. The server allocates a reference number to the transaction and it sends the reference number to the client.
4. The client sends reference number to POS2 of the merchant through NFC.
5. The POS 2 sends the reference number to the server.
6. The server checks whether all the information match and then sends the transaction status to POS 2 and the money is withdrawn from the client’s sub-wallet.

The payer can check the transaction in the history.

The merchant can check the transaction and the history in his own page on the website.

Figure 8 shows the transaction in quick payment mode between Smartphone and POS 2 with QR code:

1. The client (the payer) chooses in the application the “quick pay method” and he chooses QR code.
2. The application automatically sends a transaction request to the server.
3. The server allocates a reference number to the transaction and sends the reference number to the client.
4. The application generates a QR code from the reference number on the client’s Smartphone.
5. The POS2 of the merchant scans QR code from client Smartphone to get the reference number.
6. The POS 2 sends the reference number to the server.
7. The server checks whether all the information match and then sends the transaction status to POS 2 and the money is withdrawn from the client’s sub-wallet.

The payer can check the transaction in the history.

The merchant can check the transaction and the history in his own page on the website.

- *Towards POS2.1 (qp): with fix amount only*

Figure 9 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.1 with NFC:

1. The client (the payer) chooses in the application the “quick pay method” with NFC.
2. The application automatically sends a transaction request to the server.
3. The server allocates a reference number to the transaction and sends the reference number to the client.

4. The client's Smartphone generates a NFC in order to transfer the reference number to the POS2.1 of the merchant.
5. The POS 2.1 sends the reference number to the server.
6. The server checks whether all the information match and then sends the transaction status to POS 2.1 and the money is withdrawn from the client's sub-wallet.

The payer can check the transaction in the history.

The merchant can check the transaction and the history in his own page on the website.

- *Towards POS2.2 (qp): with fix amount only*

Figure 10 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.2 with NFC:

1. The client (the payer) chooses in the application the "quick pay method" and he chooses NFC as payment method.
2. The application automatically sends a transaction request to the server.
3. The server allocates a reference number to the transaction and sends the reference number to the client.
4. The client's Smartphone generates a NFC in order to transfer the reference number to the POS2.2 of the merchant.
5. The POS 2.2 sends the reference number to the server.
6. The server checks whether all the information match and then sends the transaction status to POS 2.2 and the money is withdrawn from the client's sub-wallet.
7. POS 2.2 is connected with printer through Bluetooth to print the ticket.

The client can check the transaction in the history.

The merchant can check the transaction and the history in his own page on the website.

Figure 11 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.2 with QR code:

1. The client chooses in the application the "quick pay method" and he chooses QR code as payment method.
2. The application automatically sends a transaction request to the server.
3. The server allocates a reference number to the transaction and sends the reference number to the client.
4. The application generates a QR code from the reference number on the client's Smartphone.
5. The POS2.2 of the merchant scans QR code from the client's Smartphone to get reference number.
6. The POS 2.2 sends the reference number to the server.
7. The server checks whether all information match and then sends the transaction status to POS 2.2 and the money is withdrawn from the client's sub-wallet.
8. POS 2.2 is connected with printer through Bluetooth to print the ticket.

The client can check the transaction in the history.

The merchant can check the transaction and the history in his own page on the website.

- *Towards another mobile device that is connected: SSPcl to SSPcl*

Figure 12 shows the transaction in direct payment mode between two smartphones with NFC.

Figure 13 shows the transaction in direct payment mode between two smartphones with QR code.

1. The client B (the beneficiary) enters in the application the amount that will be transferred by client A.
2. The client B initiates a transaction by sending the amount of the transaction to the server.
3. The server allocates a reference number to the transaction and sends the reference number to the client B.

4. The client B preparing reference number for NFC method to be sent to client A.
5. The client A (the payer) enters in the application the amount to be paid to client B.
6. The client B sends the reference number to client A through NFC (Figure 12). Or client A scans QR code from client B's Smartphone to get reference number (Figure 13).
7. The client A sends the reference number to the server.
8. The server sends confirmation to the client A.
9. The client A verifies the transaction and validates it by sending the 3 letters validation code back to the server.
10. The server verifies the data of the transaction; if successful, the server sends a success notification to client B and to client A.

- *Towards another mobile device that is not connected: SSPcl to SSPsc*

Figure 17 shows the transaction in case of P2P transfer between smartphone and non-connected phone:

1. The client B (the beneficiary) requests a reference number for the "transfer transaction via SMS" to the server by sending keyword, the amount of the transaction, and password.
2. The server validates the password and allocates a reference number for the transaction and sends it to the client B via SMS.
3. The client B sends SMS to client A (the payer) containing the reference number and the amount.
4. The client A chooses "paid using transfer in the SSP" and enters in the application the reference number and amount that have been given by the beneficiary. Then, the request is automatically sent to the server.
5. The server processes the transaction and sends the transaction resume to the payer.

6. The client A verifies the transaction and validates it by sending the 3 letters validation code to the server.
7. The server verifies the data of the transaction. If the transaction is valid and successful, the server sends a successful notification to the client A and sends a SMS to the client B.

- **In case of remote payment:**

  - *Online payment (e-commerce)*

Figure 14 shows the transaction in case of e-commerce payment.

1. The client clicks button "Pay with SSP" in the e-commerce page.
2. The website that has the plugin of SSP e-commerce sends the transaction data to the server.
3. The server allocates a reference number to the transaction and sends the reference number to SSP payment page
4. The SSP payment page generates a QR code with the reference number.
5. SSP payment page displays the QR code and the client scans the QR code with his Smartphone.
6. The client verifies the transaction and validates it with the 3 letters validation code and sends the data to the server via the application.
7. The server verifies the data of the transaction; if successful, the server sends a successful notification to the client.
8. The server sends a notification to the merchant by email.

Client's balance is debited and merchant's balance is credited.

- *SSPcl to SSPcl:*

Figure 15 shows transaction in case of P2P between two smartphones by transfer of reference number.

1. The client B (the beneficiary) enters in the application the amount that will be transferred by client A (the payer).

2. The client B requests a reference number for the transaction to the server by sending the amount of the transaction.
3. The server allocates a reference number to the transaction.
4. The server sends the reference number to the client B.
5. The client B communicates the reference number and the amount to the client A by SMS.
6. The client A receives the SMS from client B containing the reference number and the amount and he selects “Transfer Payment” in the menu of the application.
7. The client A enters in the application the reference number and amount that are communicated by the client B.
8. The client A sends the reference number and amount to the server.
9. The server processes the transaction and sends a transaction resume to the client A.
10. The client A validates the transaction by sending the 3 letters code back to the server.
11. The server verifies the data of the transaction. If the transaction is valid and successful, the server will send successful notification to the client A and to the client B.

The client A’s balance is debited and the client B’s balance is credited.

- *Transfer of money to the own bank account*

Figure 16 shows the transaction in case of bank transfer (withdrawal from client’s wallet towards client’s bank account).

1. The client chooses the bank and enter the amount has to be withdrawn and validate it using 3 letters.
2. The client fills in the data of bank transfer.
3. The server checks client's balance and his wallet is debited (with additional transfer fee if client’s bank is outside of SSP system). The SSP

billing program verifies the transaction and will then proceed to the bank transaction.

4. The server asks the bank to transfer from SSP bank account to client's bank account.
5. The SSP bank account transfers money to client's bank account.

- When the payment is generated from a non-connected mobile device:

  - *Towards POS1*

Figure 18 shows the transaction in case of transfer generated from non-connected phone to a POS 1:

1. The merchant enters in his POS1 the amount of the transaction and the phone number of the client.
2. The POS1 sends a transaction request to the server.
3. The server allocates a reference number for the transaction and sends it to POS1 and also sends the reference number and the amount that has to be paid to the client via SMS.
4. The client replies to the server by SMS containing keyword, reference number, the amount has to be paid, and his password of 3 letters and 3 numbers.
5. The server verifies the data of the transaction. If the transaction is valid and successful, the server will send a successful notification to POS1 and a SMS to the client.

The client's balance is debited and the merchant's balance is credited.

- *Towards a mobile device that is connected: SSPsc to SSPcl*

Figure 19 shows the transaction in case of transfer generated from non-connected phone to a Smartphone.

1. The client B (the beneficiary) enters in the application the amount of the transaction and the phone number of the client A (the payer).

2. The client B sends a request “getting paid by using SMS” to the server by sending the amount of the transaction and the phone number of the client A to the server.
3. The server allocates a reference number for the transaction and sends the notification and reference number to the client B and also to client A by SMS.
4. The client A replies to the server by SMS containing keyword, reference number, the amount to be paid, and his password of 3 letters and 3 numbers.
5. The server verifies the data of the transaction.
6. If the transaction is valid and successful, the server will send a successful notification to the beneficiary and a SMS to the client A.

The client A's balance is debited and the client B's balance is credited.

- *Towards a mobile device that is not connected*

Figure 20 shows the transaction in case of transfer generated between two non-connected phones.

1. The client A (the payer) sends a SMS to the server. The content of the SMS includes keyword, the phone number of the client B (the beneficiary), the amount of the transaction and his password of 3 letters and 3 numbers.
2. The server verifies the data and makes the transaction if successful.
3. The server sends a SMS notification to the client A and the client B.

The client A's balance is debited and the client B's balance is credited.

- *To a bank account*

Figure 21 shows the transaction in case of bank transfer (withdrawal from client’s wallet to client’s bank account).

1. The client sends a SMS to the server. The content of the SMS includes keyword, the amount of the transaction, and his password of 3 letters and 3 numbers.

2. The server verifies the data and makes the bank transfer request.
3. The server sends a SMS notification to the client and client' balance is debited.
4. The SSP billing program makes the transfer from SSP account to the client's bank account.
5. The SSP billing program verifies the bank transfer request and decreases the balance of the client's wallet.
6. The server sends a successful notification to the client.

C. Loading the wallet

Figure 22 shows Wallet Top up.

The client who wishes to feed his wallet must make a prior request to the server using the appropriate function in the application.

He shall state the amount he wants to pay or transfer.

The server will indicate the amount to be paid. This amount is chosen by the user, but the last 3 digits are replaced by the ones that the server chooses in order to identify the payment.

It is this amount, as specified by the server, which must be paid by the client (if the client has no bank account) or transferred from his account to the SSP account in which he has his wallet.

V. Transparency

Upon opening the application, and after logging in, the user knows the balance of his account.

After each operation, the balance is shown.

The non-commercial user receives by e-mail the monthly statement of his account. The merchant receives the daily, monthly and annual statement distributed into a principal amount, taxes and service if appropriate.

At the request of the user that communication can be done by mail.

VI. Real time

At the same time when the transaction is completed, the electronic wallet of the recipient is credited with the amount of the transaction.

This money is immediately available. It can be withdrawn, transferred or used for any payment.

If the transfer is between the banks in which SSP has an account, then it is in real time.

If the transfer is made to a bank in which SSP has no account, then the notification of the transfer is done in real time, but the recipient will not receive the money until the account has been credited by the bank.

VII. The advantages over the previous technique

Compared to previous systems, the SSP provides the following benefits:

- The money transfers are made in real time, the transferred money is immediately available.
- Safety is assured because:
    - There is no sensitive data transferred between stakeholders.
    - No sensitive data is found on the mobile device; therefore, there is no fear to make a transaction from a mobile device.
    - Total security is ensured not only by the triple authentication system and the validation, but especially thanks to the asymmetric routing, unidirectional and parallel encrypted information.
    - The asymmetric and parallel routing system prevents the trace of the source of the message and prevents hacking and phishing.
    - The main server is located in an area outside of the Internet.
    - When the transaction is made, SSP transfers its own money between the accounts so that the money of the users are never in danger.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

Figure 1 shows the Wallets organization in SSP account in a bank;

Figure 2 shows what happens when a transaction that involves two banks is on process;

Figure 3 shows what happens when a transaction within one bank is on process;

Figure 4 shows the registration proceeding;

Figure 5 shows the transaction in direct payment mode between Smartphone and POS 1 with NFC;

Figure 6 shows the transaction in direct payment mode between Smartphone and POS 1 with QR code;

Figure 7 shows the transaction in quick payment mode between Smartphone and POS 2 with NFC;

Figure 8 shows the transaction in quick payment mode between Smartphone and POS 2 with QR code;

Figure 9 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.1 with NFC;

Figure 10 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.2 with NFC;

Figure 11 shows the transaction in quick payment mode with fix amount only between Smartphone and POS 2.2 with QR code;

Figure 12 shows the transaction in direct payment mode between two Smartphone with NFC;

Figure 13 shows the transaction in direct payment mode between two Smartphone with QR Code;

Figure 14 shows the transaction in case of e-commerce payment;

Figure 15 shows transaction in case of P2P between two Smartphone by transfer of reference number;

Figure 16 shows the transaction in case of bank transfer (withdrawal from client's wallet towards third party's bank account);

Figure 17 shows the transaction in case of P2P transfer between Smartphone and non-connected phone;

Figure 18 shows the transaction in case of transfer generated from non-connected phone to a POS 1;

Figure 19 shows the transaction in case of transfer generated from non-connected phone to a Smartphone;

Figure 20 shows the transaction in case of transfer generated between two non-connected phones;

Figure 21 shows the transaction in case of bank transfer (withdrawal from client's wallet to client's bank account);

Figure 22 shows Wallet Top up;

Figure 23 shows the circuit that the encrypted data have to follow to reach the server and vice-versa following the technology of asymmetric and parallel paths. In this figure ISP stands for Internet Service Provider.

BEST WAY TO IMPLEMENT THE INVENTION

The invention consists both in the particular management of the wallets and in the protection afforded to sensitive data and to the ones that are specific to all financial transactions, either when they are in move or when at rest.

Regarding the management of wallets in order that the transfer of money operates in real time, it is necessary to open an account in different banks or financial institutions or other establishments. Each account must include the wallets of the users and money of SSP.

Regarding data protection during their transport, the functions of the mobile device have not to be used because they leave traces in the cache memory and overall it is important to forbid any transit of sensitive data during a transaction.

It is also important to prevent any possible return of data through the same path, to prevent hacking or phishing and finally a sharp cryptography system must be used.

As far as the protection of data at rest is concerned, the main server has to be protected from the outside world by building around it a powerful firewall and placing it in an area where internet cannot reach it.

INDUSTRIAL APPLICABILITY

SSP thanks to its safe system of transferring the data from a mobile device that is not safe and thanks to its way of managing the wallets of its users, permits the payment in real time at low costs and the financial inclusion of the small actors who have no bank account, who have no Smartphone but simply a phone that is not connected.

SSP is using bank accounts to place its money and the wallets of the users and therefore is using the services of the banks when a transfer of money is requested by a user to a recipient who is not a user and who has no account in a bank in which SSP has an account.

When a transfer of money is requested from a user to another user, SSP does not need to use the services of a Bank because SSP is acting as a clearing house even if the users are not in the same bank but in banks where SSP has an account.

SSP can also operate outside the actual financial institutions because its users do not need a bank account when they have a wallet.

When operating outside the actual system, SSP can work as an independent institution with its own ATM and offices.

SSP can also use existing non banking establishments with many branches / offices in all the cities of a country where users can fill their wallet or withdraw money.

CLAIMS

1. A method for transferring money from any mobile device from a plurality of users to a plurality of recipients, including all steps of the transfer and of the payment as from the time the order is given till the time the money is received.
2. The method of claim 1 wherein financial transactions are made without bank card, debit or credit card.
3. The method of claim 1 wherein the mobile device that is used to give the order of transfer is connected to internet.
4. The method of claim 1 wherein the recipient is also using a mobile device that is connected to internet.
5. The method of claim 1 wherein there is no application in the mobile device but only an interface.
6. The method of claim 1 wherein the user is not using the tools of the mobile device to enter any data but the virtual keyboard of the SSP system.
7. The method of claim 1 wherein the personal data of the user are sent to the server when registering and kept into the server so no trace of them can be found in the cache memory of the mobile device.
8. The method of claim 1 wherein the personal data of the user are never used in any transaction.
9. The method of claim 1 wherein the user when registering is opening a wallet in the account of SSP in the bank where he has also an account.
10. The method of claim 1 wherein the user when registering is opening a wallet in the account of SSP in a bank where SSP has an account even if he has no account in such bank.
11. The method of claim 1 wherein the user when registering is openinga wallet in the account of SSP without referring to any bank and wherein the user does not put money in a bank account or transferring money to a bank account but only in his wallet.

12. The method of claim 1 wherein the user has to request from the server the authorization to fill his wallet of the amount of his choice.

13. The method of claim 1 wherein the server is giving such authorization but for an amount where the 3 last figures that are chosen by the server permit to identify the user.

14. The method of claim 1 wherein the user has to fill his wallet with the amount that the server has indicated to him.

15. The method of claim 1 wherein each of the parties in a direct transaction has to contact separately the server and indicate the amount that has to be paid (for the payer) and the one that has to be received (for the recipient).

16. The method of claim 1 wherein upon reception of the information contained in claim 15 the server is making a record, allocating a reference number to the transaction.

17. The method of claim 16 wherein the record contains all the data of the transaction including the reference number.

18. The method of claim 16 wherein the reference number will always been kept by the server in the archives of the transactions.

19. The method of claim 1 wherein the server is sending the reference number to the recipient of the transaction.

20. The method of claim 1 wherein the recipient of the transaction can be a vendor or any beneficiary.

21. The method of claim 1 wherein the recipient is only transferring the reference number of the transaction to the payer using each a mobile device, by means of Near Field Communication, 'NFC' or QR code scanning.

22. The method of claim 1 wherein the reference number is automatically sent by the mobile device of the payer to the server.

23. The method of claim 1 wherein if the server does not receive the reference number from the payer the transaction is cancelled.

24. The method of claim 1 wherein upon reception of the reference number from the payer the Server is sending to the payer a request of validation of the amount that has to be paid.

25. The method of claim 1 wherein once the validation code of 3 letters is entered and correct, the server is completing the transaction, sending a notification to each party with the actual situation of their respective wallet.

26. The method of claim 1 wherein at the real time the notification is received by the recipient the money is available and can be withdrawn or transferred or used to make any payment.

27. The method of claim 1 wherein there is a triple degree of authentication control, namely the telephone number and the IMEI which are controlled automatically by the server and the ID that the user must have inserted.

28. The method of claim 27 wherein the ID consists in a 6 digit code of 3 letters and 3 figures.

29. The method of claim 1 to wherein there is a triple validation system, i.e. the correspondence between the amounts reported separately, the return of the reference number of the transaction by the second party to the transaction and the validity of the validation codes.

30. The method of claim 29 wherein the validation of the transaction is made by a 3 letters code.

31. The method of claim 1 wherein each party only communicates with the server separately and the only connection between them, when it is required, is only to transmit the number that the server has assigned to the transaction.

32. The method of claim 1 wherein the contact system between users and the server is that of an asymmetric and parallel path.

33. The method of claim 1 wherein any data sent by a user to the server is using a one way channel, the server using another way to enter into contact with the user.

34. The method of claim 1 wherein any direct transaction is made in parallel ways, each party being only in contact with the server.

35. The method of claim 1 wherein all data are automatically encrypted before being sent.

36. The method of claim 1 wherein the payer can make any transfer or any transaction to any account in any bank or any institution or any virtual account or any wallet in any country or online payment from his wallet by requesting the server to complete such transaction.

37. The method of claim 1 wherein the user is making a transaction from a mobile device that is not connected to internet.

38. The method of claim 1 combined with claim 37 wherein the user is opening a sub-wallet of which he can fix the number of transactions that can be made by day, the maximum amount of each transaction and the total amount that can be spent in one day.

39. The method of claim 37 wherein the user has to request by SMS the authorization of the server before filling in his sub-wallet of the amount of his choice.

40. The method of claim 37 wherein the server is giving such authorization but for an amount where the 3 last figures that are chosen by the server permit to identify the user.

41. The method of claim 37 wherein the user has to fill his wallet with the amount that the server has indicated to him.

42. The method of claim 37 wherein the user can have a sub-wallet even if he has no bank account, the server indicating him the bank in which SSP has an account where the payment has to be made or where the payment can be made even if not in a bank.

43. The method of claim 37 wherein the user can make any financial transaction from his sub-wallet by means of SMS sent to the server requesting the

authorization and validating the order with only one code of 6 digits (3 letters and 3 figures).

44. The method of claim 1 wherein the server is operating as a clearing house in order to make the transaction in real time.

45. The method of claim 1 wherein when receiving from a user an order of payment to another user in another bank where SSP has an account, the server is debiting the wallet of the said user crediting SSP of the same amount in the same account, same bank while in the other bank the server is crediting the wallet of the recipient and debiting SSP's one of the same amount.

46. The method of claim 1 wherein when receiving from a user an order of payment to another user in the same bank, the server is debiting the wallet of the said user crediting SSP's one of the same amount while the server is crediting the wallet of the recipient and debiting SSP's one of the same amount.

47. The method of claim 1 wherein when being requested to make a transfer to another bank in which SSP has no account, the server is debiting the wallet of the user and crediting SSP's one of the same amount and sending the bank an order to transfer the money.

48. The method of claim 1 wherein the user is making a direct payment from a mobile device, connected or not connected, to a POS that is part of SSP system, transmitting the reference number by means of NFC, QR Code or SMS.

49. The method of claim 48 wherein the POS is directly connected to the server and is communicating with the server using a one way and parallel path, all data being automatically encrypted before being sent.

50. The method of claim 1 combined with claim 36 wherein the user is making a direct payment from a mobile device that is not connected, to a POS that is part of SSP system, transmitting the reference number by means of SMS.

51. The method of claim 1 wherein the user is making a quick payment from a mobile device that is connected, to a POS that is part of SSP system, transmitting the reference number by means of NFC or QR Code.

52. The method of claim 51 combined with claim 44 wherein the server is debiting the sub-wallet of the payer while crediting the wallet of the vendor.

53. The method of claim 51 wherein the server is transmitting the reference number to the payer using a one way and parallel path, the reference number being encrypted before being sent.

54. The method of claim 51 wherein the server is sending the reference number to the payer of the transaction.

55. The method of claim 51 wherein the payer is only transferring the reference number of the transaction to the POS by means of Near Field Communication, 'NFC' and QR Code.

56. The method of claim 51 wherein the reference number is automatically sent by the POS to the server.

57. The method of claim 51 wherein if the server does not receive the reference number from the POS the transaction is cancelled.

58. The method of claim 1 wherein the user can withdraw money from an ATM.

59. The method of claim 58 wherein before the user withdraws money from the ATM, the user must request the withdrawal of money to server, then the server will send the reference number to the user.

60. The method of claim 58 wherein before the user withdraws money from the ATM, the user must request the withdrawal of money to server, then the server will send the reference number to the user by SMS if the mobile device of the user is not connected.

61. The method of claim 58 wherein the user is choosing SSP on the screen as way to withdraw money.

62. The method of claim 58 wherein the user is typing upon request his phone number.

63. The method of claim 58 wherein the user is typing upon request his 6 digit authentication code.

64. The method of claim 58 wherein the user is choosing the amount he wants to withdraw.

65. The method of claim 58 wherein the ATM is sending to the server the data given by the user.

66. The method of claim 58 wherein upon request from ATM the user is typing the reference number that he has received.

67. The method of claim 58 wherein the ATM is sending to the server the reference number that has been typed by the user.

68. The method of claim 58 wherein the server is sending to the ATM the authorization to complete the transaction.

69. The method of claim 58 wherein the user is receiving his money and notification of the new balance of his wallet or sub-wallet.

70. The method of claim 1 wherein the server is not connected to internet.

71. The method of anyone of claim 1 to 70 where the word wallet means a subaccount and sub-wallet a limited subaccount.

AMENDED CLAIMS
received by the International Bureau on 24.11.2016

CLAIMS

1. A method of making a financial transaction (either direct online payment or payment between two or more users) or withdrawal of money in REAL TIME, which means that the transfer of money occurs at the second the transaction or withdrawal order is executed, without the use of any credit or debit card from any mobile device from a plurality of payers to mobile or fix devices (such as a POS - Point of Sales) of a plurality of recipients (beneficiaries or vendors), without contact, using NFC, QR code or SMS, in total security and a method of management of wallets and /or sub-wallets linked to each of the users and/or recipients including the following steps and characteristics :
    a. A financial transaction can be an order of payment that has to be executed from a bank account to another bank account avoiding the transfer of cash money.
        i. A financial transaction may involve only one user when the user is buying online a product of SSP (Secure System of Payment). A financial transaction may involve several users when a user is transferring money to another user. In that case users can be named the parties at a transaction or each party at a transaction;
        ii. A transaction starts from the moment a user is opening his application requesting the accomplishment of a transaction by clicking on the appropriate button giving an order to the server till the time the order is executed by the SERVER (when not specified the term SERVER or SSP SERVER or server or SSP server means the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) and that the SERVER has sent, through Server OUT, to each party at the transaction a message saying that the transaction has been successful or cancelled. This last communication of the SERVER is called “notification”;

iii. The notification contains the amount of money that the user had on his wallet before the transaction, the amount of money of the transaction and the amount of money that is in the user's wallet after the transaction. Such amount is the new balance;

b. To be able to use SSP system and make transactions, a user has to transfer money to the wallet or sub-wallet that has been opened for him when registering :

i. The words wallet means a subaccount in the bank account of SSP and sub-wallet a limited subaccount in the bank account of SSP;

ii. A wallet is created for each user that is making the transaction from a connected mobile device and who owns a bank account;

iii. A sub-wallet is created for each user that is making the transaction from a connected mobile device and who owns a bank account and who wants to make quick payment;

iv. A quick payment takes place when the user has to pay a low amount of money in an urgent situation by just passing the mobile phone in front of the POS quick payment (like for paying in a bus);

v. A sub-wallet is also created for each user who is using a non connected mobile device to make a financial transaction;

vi. The user, in order to top up (refill his wallet or sub-wallet), has to request from the Server the authorization and communicate the amount of money he wants to transfer;

vii. The Server will change the 3 last digit of the amount of money that the user wants to transfer, i.e., if the user wants to transfer 100.000IDR the Server will give the authorization for transferring 100.456IDR. This is the amount of money that the user has to transfer in place of the 100.000IDR. The amount

that will be available in the wallet or sub-wallet of the user is the one that the SERVER has indicated and not the one that the user wanted initially transfer;

c. The security is inherent to the system because :

i. The application is not in the mobile device but in SSP server which is out of contact with the outside world (internet) :

1. The central piece of the system is SSP Server that is managing all the system from the time an order of payment is given from a mobile device using INTERNET or a SIM CARD till the time the order is executed while NOT IN CONTACT WITH INTERNET and without any connection with any phone line: SSP Server is totally isolated;
2. The SERVER is assisted by the following auxiliary servers: server system, several database servers and several back up servers which are all out of contact with the outside world: they are totally isolated;
3. Only the servers IN and OUT are in contact with internet and it is through the servers IN and OUT that the SERVER can communicate with the outside world;
4. Only the SERVER is communicating with SERVER IN and SERVER OUT by private and totally secure canals. The other servers that assist the main one are only communicating by private channels with the SERVER;
5. One of the database servers (with its backup server) is only dedicated to keep trace of all the transactions (order given that is executed or not) that have been initiated and which are named archives when the file that has been opened for such transaction is closed;
6. The file created for a transaction is open until the order of the transaction has been executed or until the time SSP

Server has cancelled the transaction and that the users have received notice (notification) of it;

ii. In the mobile device there is only an interface including its own keyboard so that the keyboard of the device is never used :

1. The system includes the use of any mobile device just as a mirror, that contains no data about the user and in which the user cannot input any data;
2. For that reason in the mobile device of the user there is only an interface using its own keyboard, so the user is not using the keyboard of the device. The keyboard of the interface is therefore named virtual. If using the keyboard of the device, the device will keep what is typed in its memory (which is the cache memory of any mobile device);
3. For that reason, each time the user is typing a digit or a letter, using the virtual keyboard, it is automatically sent to the SERVER, one by one and encrypted;
4. For that reason, the user is giving, only when registering, his personal data which are referring to his identity (first and family names, address, date and place of birth, phone number and email address, and account number for the user who is a merchant). The non merchant user is never communicating his bank account. The bank account of the user will be automatically known by the SERVER when filling the wallet or sub-wallet for the first time. Such data are the sensitive data that are never used for any transaction;

iii. Strong authentication and strong validation :

1. The SSP system is using a strong authentication and validation system.

2. Authentication is the way the SERVER can know that the one who is giving an order or who is receiving a payment is really the one who can do it.
3. Authentication is using the telephone number of the user, the IMEI (International Mobile Equipment Identity) of the device the user is using and a six digit password. This six digit password (3 letters and 3 digits) is named the ID of the user.
4. Validation is the way that the SERVER can be sure that the payer really wants to pay the amount of money that has been communicated to the server.
5. For that reason, the authentication code is different from the validation code.
6. Authentication code is made from 3 letters and 3 digits.
7. Validation code is made from 3 letters.
8. Both Authentication and Validation codes are chosen by the user when registering.

iv. Secure architecture of the system :

1. The architecture of the system, which is also named the contact system, is parallel and asymmetric.
2. It is parallel because when the user who is giving the order is making a transaction he is in contact with the SERVER only, while the user who has to receive the payment is also in contact with the SERVER only.
3. The SERVER is in contact with each party to the transaction (payer or beneficiary) in a separate path: in parallel.
4. The only contact that will take place to finalize the transaction is when the beneficiary of the payment, who has received from the SERVER the file number (also called reference number) that the SERVER has open

for the transaction, is communicating it to the payer using NFC or QR code or SMS.

5. The payer, the one who is giving an order of payment, still using the virtual keyboard, has to type the amount of money he wants to pay.
6. It is only when the SERVER is receiving back the file number (also named reference number) with the amount of the transaction and when such amount is corresponding to the one the beneficiary has given, that the transaction is made. The amount of the transaction together with the file number, the authentication and validation are the information the SERVER needs to finalize a transaction.
7. In case the SERVER does not receive the file number or should the amount of money to be paid not correspond, the transaction is cancelled.
8. It is asymmetric because the channel used by any user to communicate to the SERVER is not the one that the SERVER is using for communicating with the users.
9. For that reason the communication coming from the user is arriving to an auxiliary server named SERVER IN which is at the border of the outside world, the one in contact with internet.
10. For that reason the communication going to the user is leaving from another auxiliary server named SERVER OUT which is at the border of the outside world, the one in contact with internet.
11. The SERVER is out of contact with the outside world: It only communicates with Server IN and Server OUT by a private channel.

12. The advantage of such system is that it forbids any hacking and any fishing.

d. The speed of transfer is the second component inherent to the system thanks to the management of the wallets :

1. The SSP system is also including the management of wallets.
2. When someone is registering in SSP, he automatically receives an account number which is named wallet or sub account: it is an account in one of the bank accounts of SSP.
3. In the banks with which SSP is working, SSP has opened a SSP account.
4. This SSP account is divided in as many subaccounts as many users who have an account in the same bank. This SSP account contains also the money of SSP and that SSP will use to execute the transactions without transferring any money from one bank to another one.
5. When registered the “someone” becomes a user. The user is named payer or beneficiary/vendor following the user is paying or receiving money.
6. When giving an order of payment, the order is received by SSP Server. SSP Server is verifying the reality of the transaction and the feasibility (identity of the parties, sufficient amount of money in the wallets and compliance with the law relating to the money laundry). Then SSP Server is executing the order.
7. To execute the order, SSP does not need any interference from a bank as it operates as a clearing house, having sufficient money in each of his accounts to this purpose.

8. When a user wants to pay, in the SSP account his wallet is diminished for the amount of money that has to be transferred and the money of SSP in his account is increased by the same amount of money, while in the SSP account in the bank of the beneficiary the money of SSP is going down and the wallet of the beneficiary is increased of the same amount of money.
9. The wallets of the parties to a transaction (payer(s) and beneficiary(ies)) can be in the same bank or in different banks. Therefore when a payment is made between 2 users or more having their wallets in the same bank, the transfer is immediate in the same bank account of SSP between the 2 subaccounts (wallets), without any intervention of the bank.
10. When the 2 users or more have their wallets in different banks, the system is that the wallet of the payer is diminished by the amount of money that he is paying while the part of SSP in SSP bank account is increased and at the same time, in the other(s) bank(s), the wallet(s) of the beneficiary(ies) (the ones who receive the money) is/are increased by such amount and the part of SSP in SSP bank account in the bank(s) of the beneficiary(ies) is diminished by the same amount of money, without any intervention of the banks.
11. Therefore there is no direct connection between the users and the banks.
12. Therefore the transaction can take place in real time that means at the second the payment is made, even when a transaction is made between wallets that are opened in different banks.

2. The method of claim 1 wherein the mobile device that is used to give the order of transfer/payment is either connected to internet or not.

3. The method of claim 1 wherein the recipient (beneficiary or vendor) is also using a mobile device that is connected to internet.

4. The method of claim 1 where the user does not need to have a bank account to register in the SSP system: if he has, his wallet or sub-wallet will be opened in the SSP account placed in the same bank; if not, his wallet or sub-wallet will be opened in one of the SSP account, at the discretion of SSP.

5. The method of claim 4 where, to be able to use SSP system and make transactions, a user has to transfer money to the wallet or sub-wallet that has been opened for him when registering, either from his own bank account, or from an ATM device.

6. The method of claim 1 wherein the user has to request from the SERVER the authorization to fill the wallet of the amount of money the user wants.

7. The method of claim 1 wherein the server is giving such authorization (the authorization to fill the wallet of the amount of money the user wants) but for an amount of money where the 3 last digits that are chosen by the SERVER permit to identify the user.

8. The method of anyone of claim 1 or 7 wherein the user has to fill the wallet with the amount of money that the SERVER has indicated to the user.

9. The method of claim 1 wherein each of the parties in a direct transaction (payer and beneficiary) has to contact separately the SERVER and indicate the amount of money that has to be paid (for the payer) and the one that has to be received (for the recipient).

10. The method of claim 9 wherein upon reception of the information sent by each user (respectively the amount of money that has to be paid - for the payer - and the amount of money that has to be received - for the beneficiary -), the SERVER (which unless otherwise specified is always the main server of the system) is making a record, allocating a reference number to the transaction,

the SERVER communicating with the outside world only through the servers IN and OUT.

11. The method of claim 10 wherein the record contains all the data of the transaction including the reference number.

12. The method of claim 10 wherein the reference number of the transaction will always been kept by the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) in the archives of the transactions, being the data of every transaction kept in the SSP database server after a transaction file has been closed.

13. The method of claim 1 wherein the SERVER is sending the reference number of the transaction to the recipient of the transaction (beneficiary).

14. The method of claim 1 wherein the recipient of the transaction can be a vendor or any beneficiary.

15. The method of claim 1 wherein the recipient is only transferring the reference number of the transaction as generated and sent to him by the SERVER to the payer using each a mobile device, by means of Near Field Communication, 'NFC' or QR code scanning.

16. The method of claim 1 wherein the reference number received by the payer from the beneficiary is automatically sent by the mobile device of the payer to the SERVER.

17. The method of claim 1 wherein if the SERVER does not receive the reference number of the transaction from the payer the transaction is cancelled.

18. The method of claim 1 wherein upon reception of the reference number of the transaction from the payer the SERVER is sending to the payer a request of validation of the amount of money that has to be paid.

19. The method of claim 1 wherein once the validation code of 3 letters is entered and correct, the SERVER is completing the transaction, sending a notification to each party with the actual situation of their respective wallet.

20. The method of claim 1 wherein at the second the notification (message from the SERVER saying that the transaction has been successful) is received by the recipient, the money is available and can be withdrawn or transferred or used to make any payment; this is called payment in real time.

21. The method of claim 1 wherein there is a triple degree of authentication control, namely the telephone number of the user and the IMEI (International Mobile Equipment Identity) which are controlled automatically by the SERVER and the ID (six character password of 3 letters and 3 digits) that the user must have inserted.

22. The method of claim 21 wherein the ID consists in a 6 character code of 3 letters and 3 digits.

23. The method of claim 1 wherein there is a triple validation system, i.e. the correspondence between the amounts (to be paid and to be received) reported separately by the payer and the beneficiary to the SERVER, the correct communication of the reference number of the transaction between the beneficiary (receiving it from the server) and the payer (receiving it from the beneficiary and sending it back to the server) and the validity of the validation codes.

24. The method of claim 23 wherein the validation of the transaction is made by a 3 letters code chosen by the user at the time of his registration in the SSP system.

25. The method of claim 1 wherein all data are automatically encrypted before being sent.

26. The method of claim 1 wherein the payer can make any transfer or any transaction to any account in any bank or any institution or any virtual account or any wallet in any country or online payment from the wallet by requesting the SERVER to complete such transaction.

27. The method of claim 1 where, when the user is making a transaction from a mobile device that is not connected to internet, the user is opening a sub-wallet

of which he can fix the number of transactions that can be made by day, the maximum amount of money that can be paid in each transaction and the total amount of money that can be spent in one day.

28. The method of claim 27 wherein the user has to request by SMS the authorization of the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) before filling in the sub-wallet of the amount of money that the user wants to fill in (top up). By giving the authorization, the SERVER will replace the three last digits of the amount of money suggested by the user by a combination of three digits that are chosen by the SERVER as to identify the user. The user has to fill the sub-wallet with the amount of money that the SERVER has indicated to the user, i.e., if the user wants to transfer 100.000IDR the Server will give the authorization for transferring 100.456IDR. This is the amount of money that the user has to transfer in place of the 100.000IDR. The amount that will be available in the wallet or sub-wallet of the user is the one that the SERVER has indicated and not the one that the user wanted initially transfer;

29. The method of claim 28 wherein the user can have a sub-wallet even if he has no bank account, the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) indicating to the user the bank in which SSP has an account where the payment has to be made or where the payment can be made even if not in a bank.

30. The method of claim 29 wherein the user can make any financial transaction from his sub-wallet by means of SMS sent to the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) requesting the authorization and validating the order with only one code of 6 characters (3 letters and 3 digits).

31. The method of claim 1 wherein when being requested to make a transfer to another bank in which SSP has no account, the SERVER is debiting the wallet

of the user and crediting SSP's one of the same amount of money and sending the bank an order to transfer the money.

32. The method of claim 1 wherein the user is making a direct payment from a mobile device, connected or not connected, to a POS (Point of Sale) that is part of SSP system, transmitting the reference number by means of NFC, QR Code or SMS.

33. The method of claim 32 wherein the POS is directly connected to the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) and is communicating with the SERVER using a one way and parallel path, all data being automatically encrypted before being sent.

34. The method of claim 26 wherein the user (payer) is making a direct payment from a mobile device that is not connected, to a POS (Point of Sale) that is part of SSP system, transmitting the reference number of the transaction sent to the payer by the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) by means of SMS.

35. The method of claim 1 wherein the user (payer) is making a quick payment from a mobile device that is connected, to a POS (Point of Sale) that is part of SSP system, transmitting the reference number of the transaction (given to the payer by the SERVER via the SSP application) by means of NFC or QR Code to the POS.

36. The method of claim 35 wherein the server is debiting the sub-wallet of the payer while crediting the wallet of the vendor.

37. The method of claim 35 wherein the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) is transmitting the reference number of the transaction to the payer using a one way and parallel path, the reference number being encrypted before being sent.

38. The method of claim 35 wherein the reference number is automatically sent by the POS to the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world). If the SERVER does not receive the reference number from the POS the transaction is cancelled.

39. The method of claim 1 wherein the user can withdraw money from an ATM, by choosing SSP on the screen of the ATM as a way to withdraw money.

40. The method of claim 39 wherein before the user withdraws money from the ATM, the user must request the withdrawal of money and the amount of money he wants to withdraw to SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world), then the SERVER will send the reference number of the withdrawal to the user either via the application if the mobile device of the user is connected or by SMS if the mobile device of the user is not connected.

41. The method of claim 39 wherein, upon request of the ATM, the user is typing his phone number on the ATM.

42. The method of claims 39 wherein the user is typing on the ATM upon request the 6 character (3 letters and 3 digits) authentication code used by SSP system to identify the user (called the ID of the user).

43. The method of claim 39 wherein the user is typing on the ATM the reference number of the withdrawal sent to the user by the server (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world)

44. The method of claim 39 wherein the ATM is sending to the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) the data given by the user, requesting the amount of money that will be withdrawn.

45. The method of claim 39 wherein the SERVER (the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the

outside world) is sending to the ATM the authorization to complete the transaction on the amount of money that was requested by the user.

46. The method of claim 39 wherein the user is receiving his money and notification (message sent by the server, being the Main Server of SSP, assisted by the auxiliary servers IN and OUT for any communication with the outside world) of the new balance of his wallet or sub-wallet (being the new amount of money that is in the user's wallet after the transaction).

47. The method of anyone of claim 1 to 46 where the word wallet means a subaccount and sub-wallet a limited subaccount.

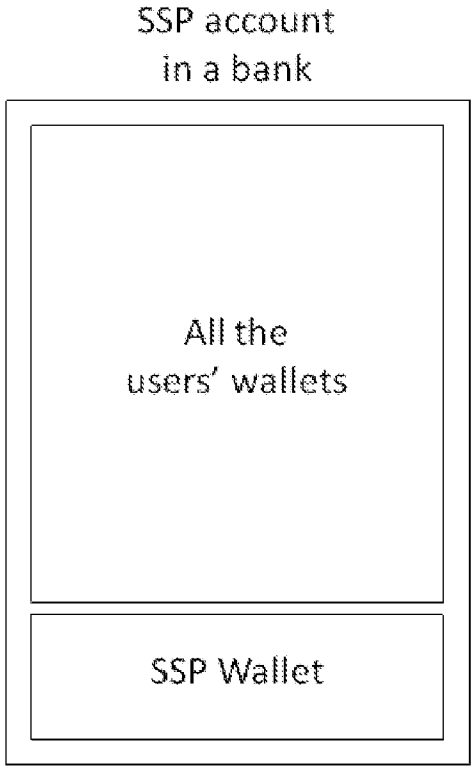


FIG. 1

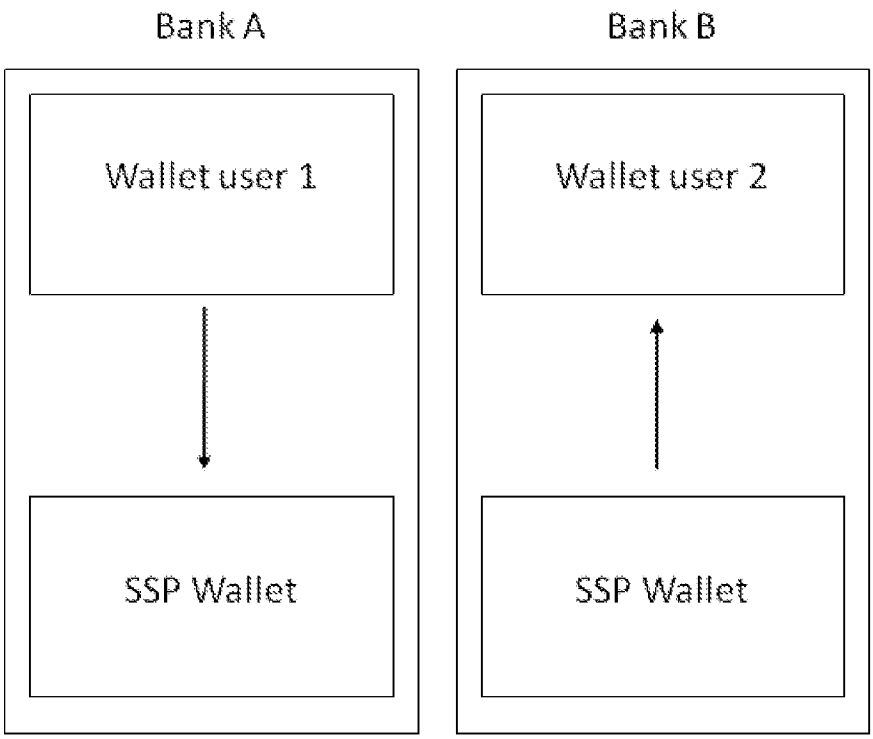

Bank A
Bank B
Wallet user 1
Wallet user 2
SSP Wallet
SSP Wallet

FIG. 2

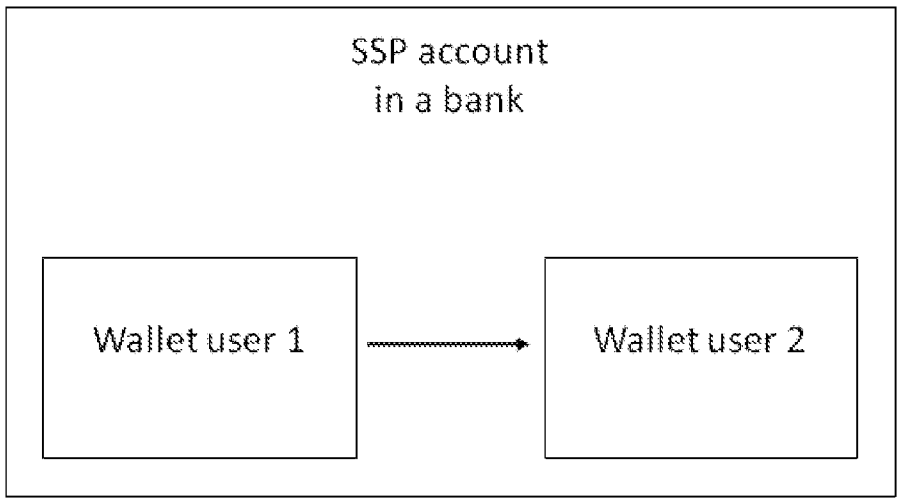


FIG. 3

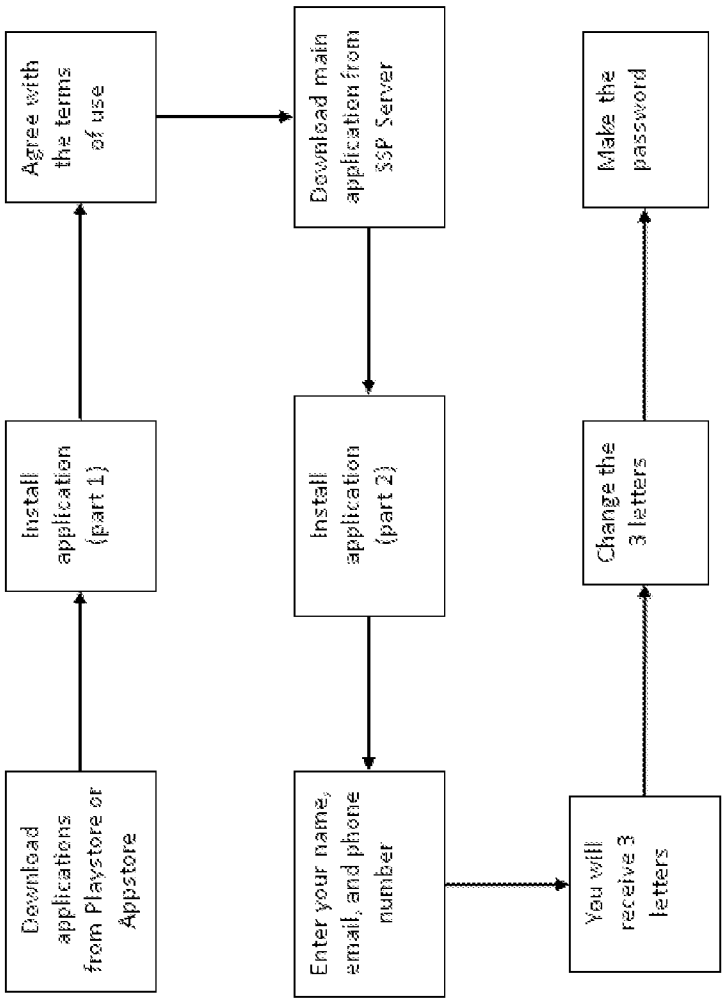

Download applications from Playstore or Appstore
Install application (part 1)
Agree with the terms of use
Download main application from SSP Server
Install application (part 2)
Enter your name, email, and phone number
You will receive 3 letters
Change the 3 letters
Make the password

FIG. 4

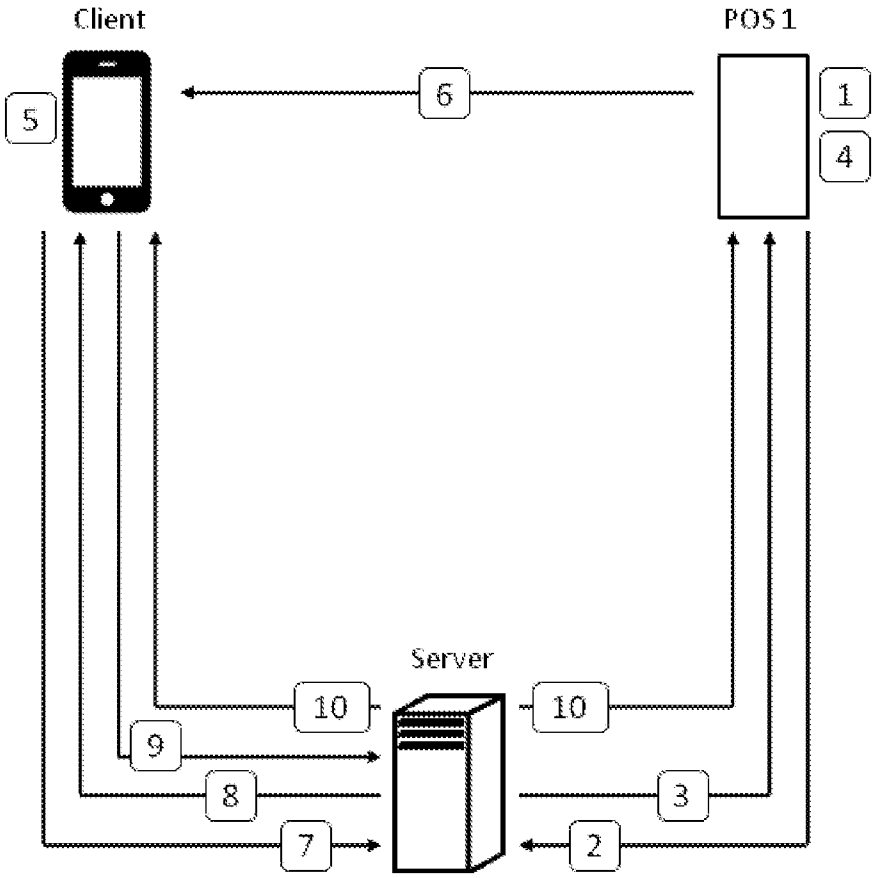


FIG. 5

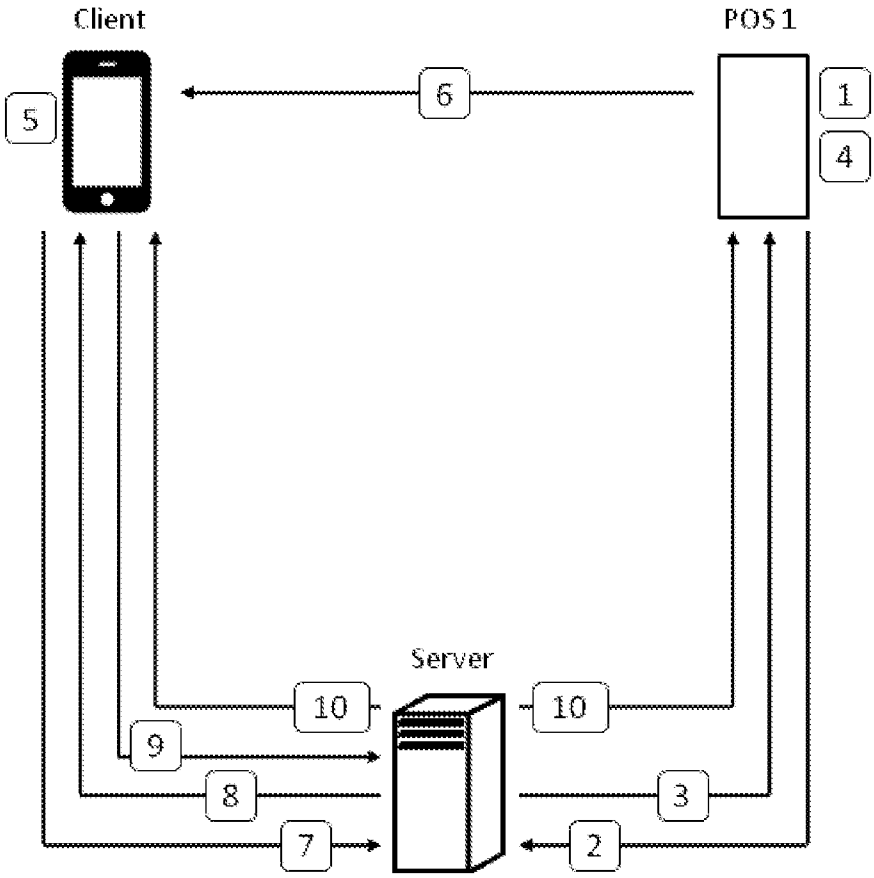


FIG. 6

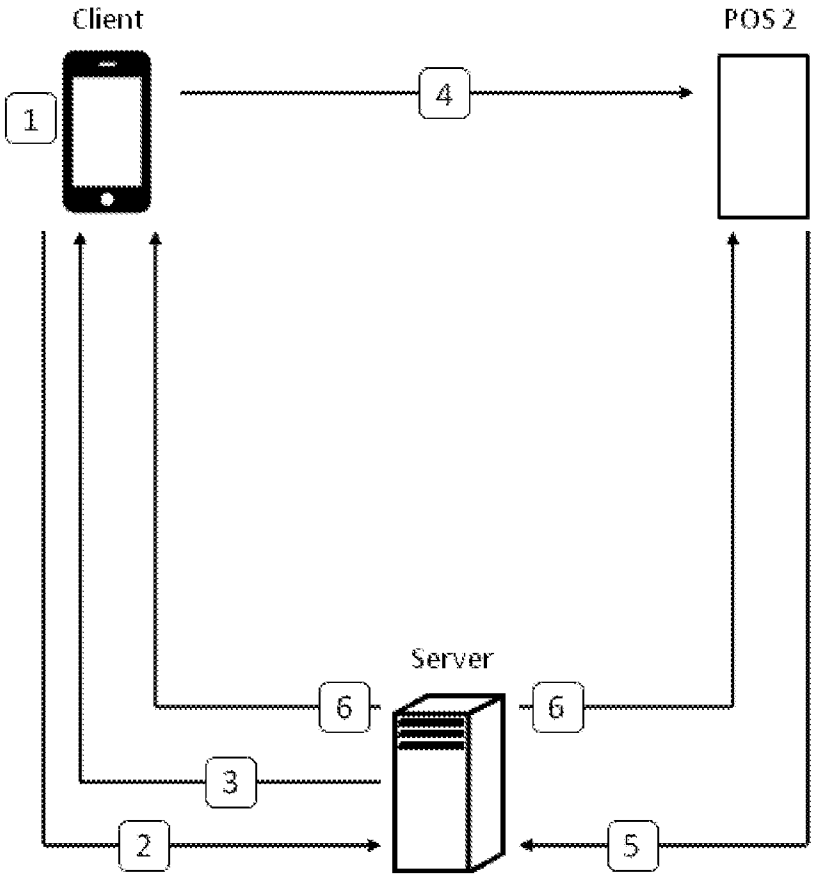


FIG. 7

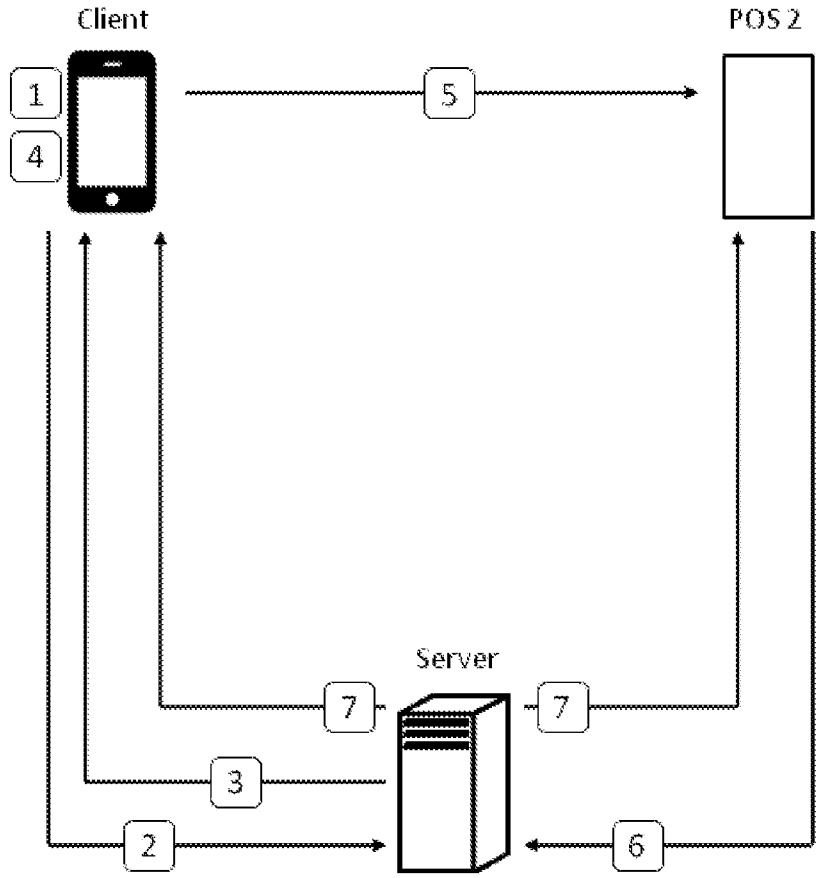


FIG. 8

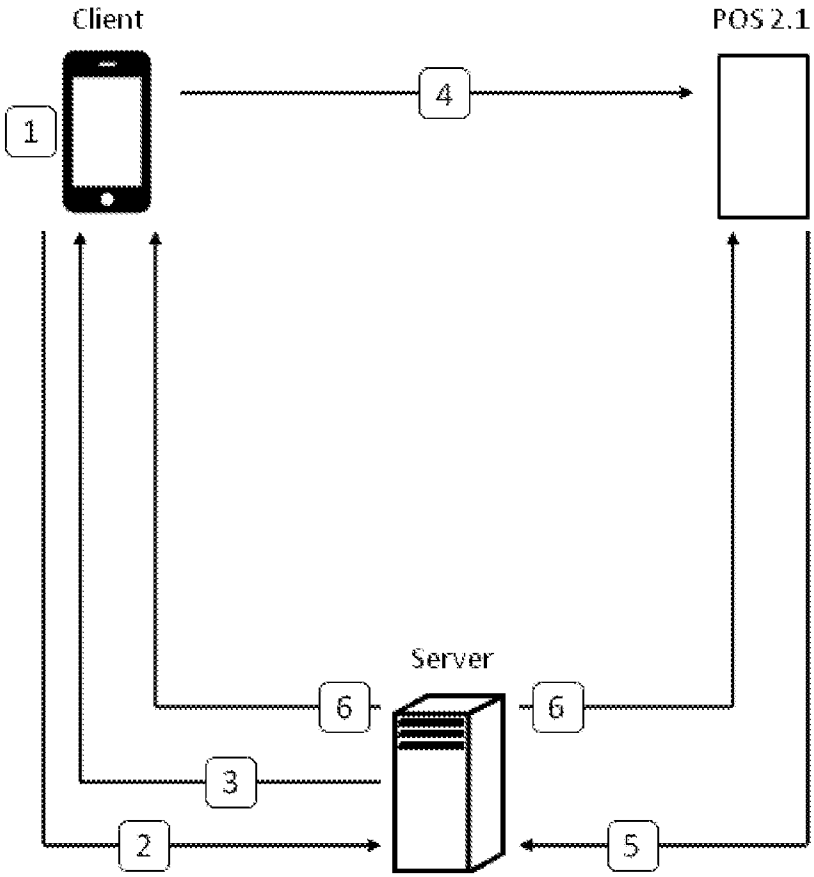


FIG. 9

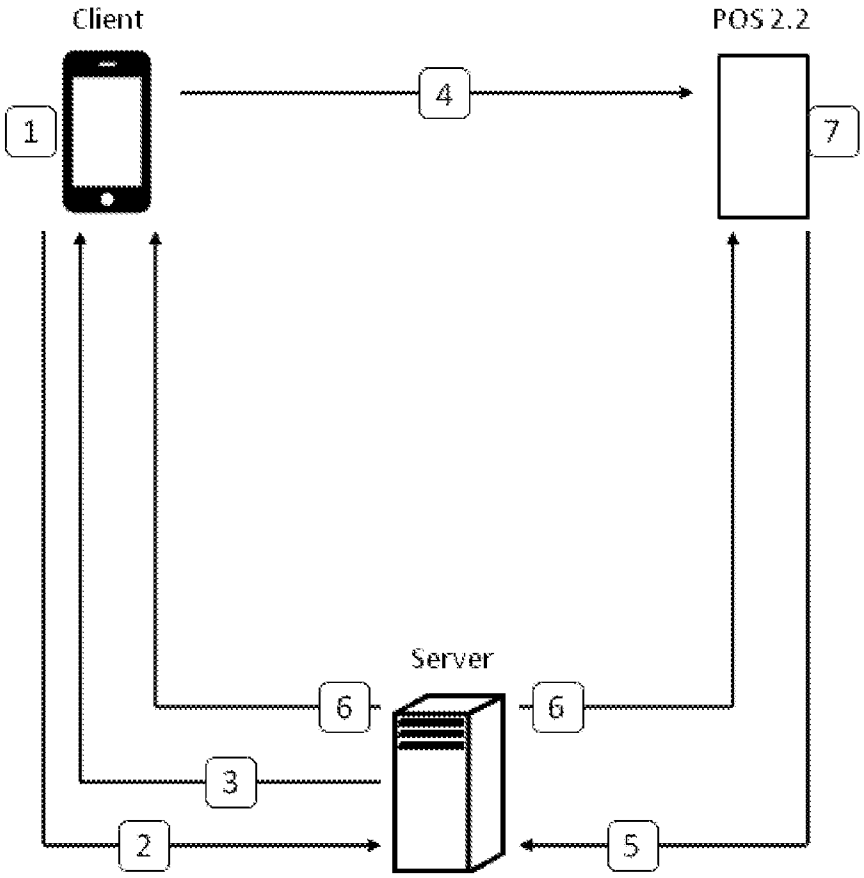


FIG. 10

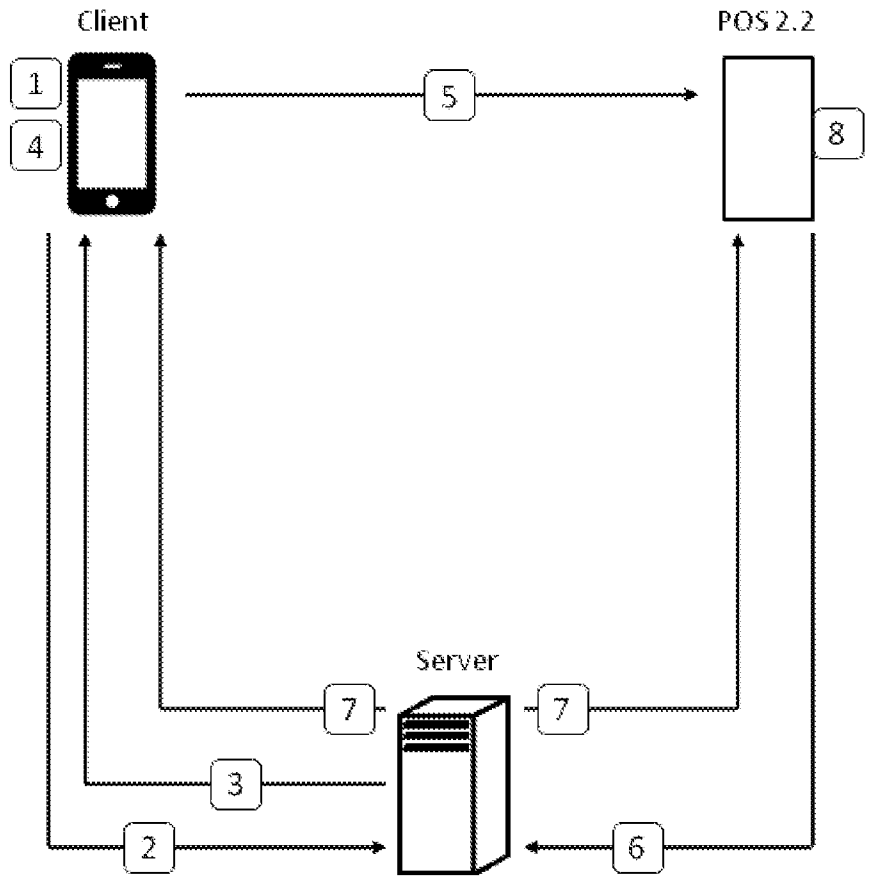


FIG. 11

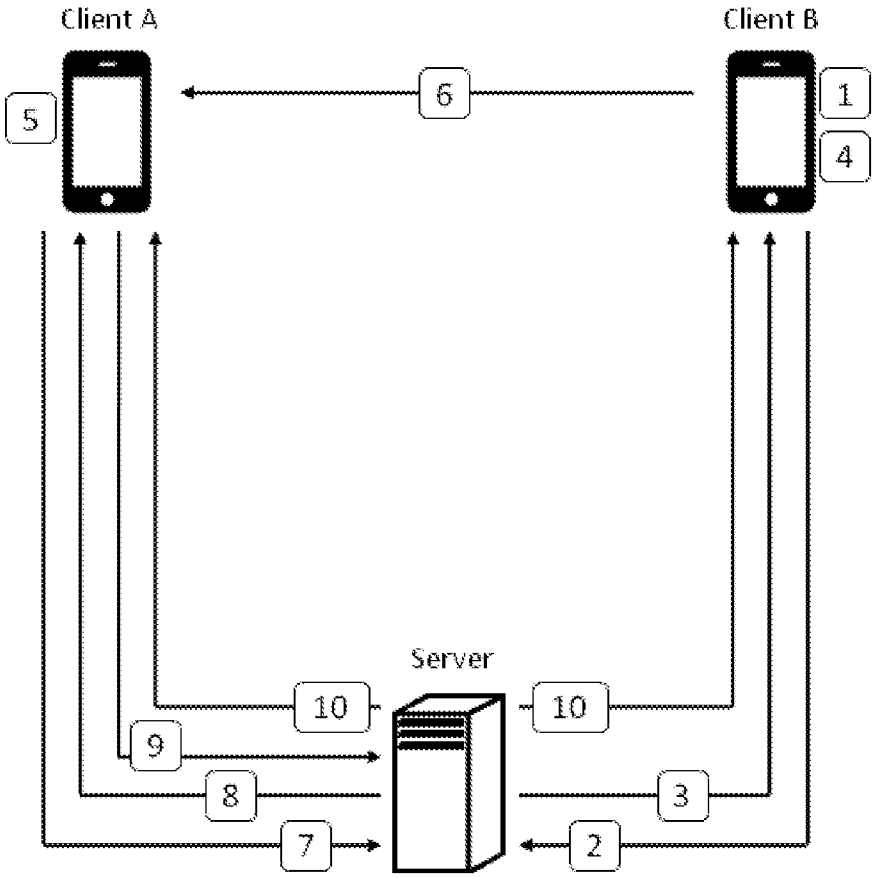


FIG. 12

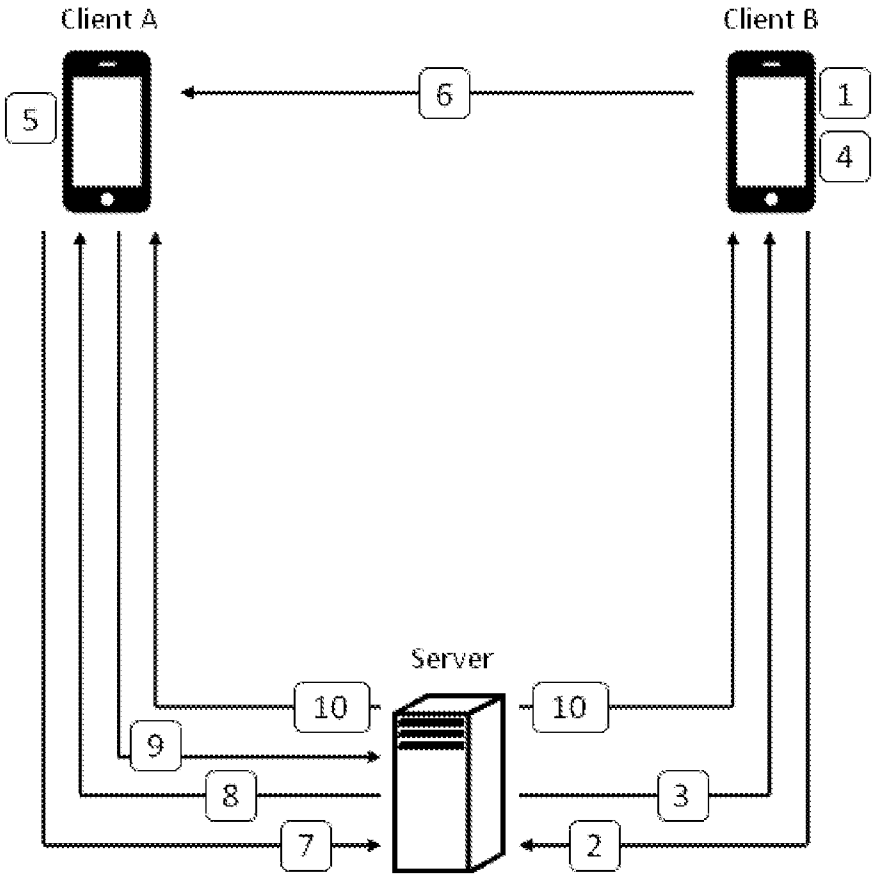


FIG. 13

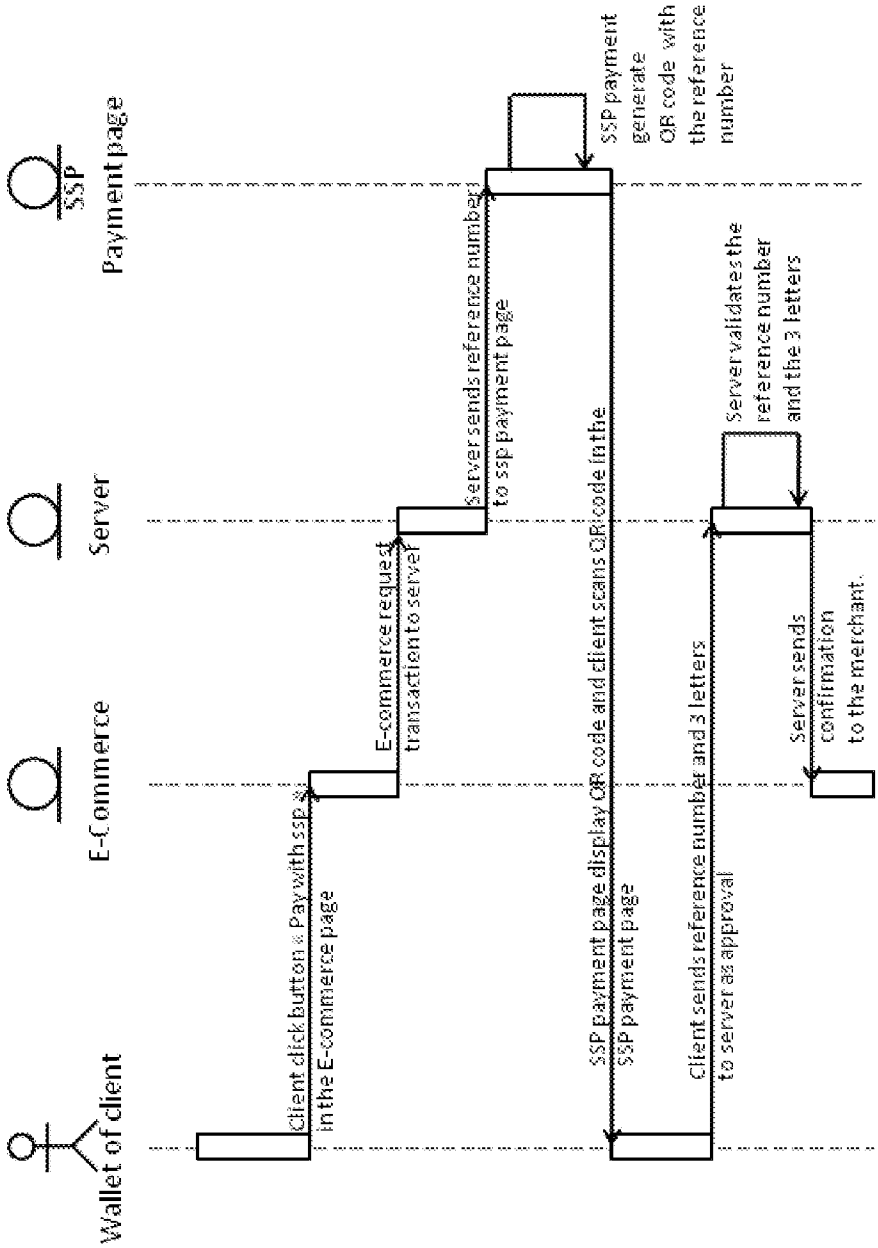

Wallet of client
E-Commerce
Server
SSP
Payment page
Client click button « Pay with ssp »
in the E-commerce page
E-commerce request
transaction to server
Server sends reference number
to ssp payment page
SSP payment
generate
QR code with
the reference
number
SSP payment page display QR code and client scans QR code in the
SSP payment page
Server validates the
reference number
and the 3 letters
Client sends reference number and 3 letters
to server as approval
Server sends
confirmation
to the merchant.

FIG. 14

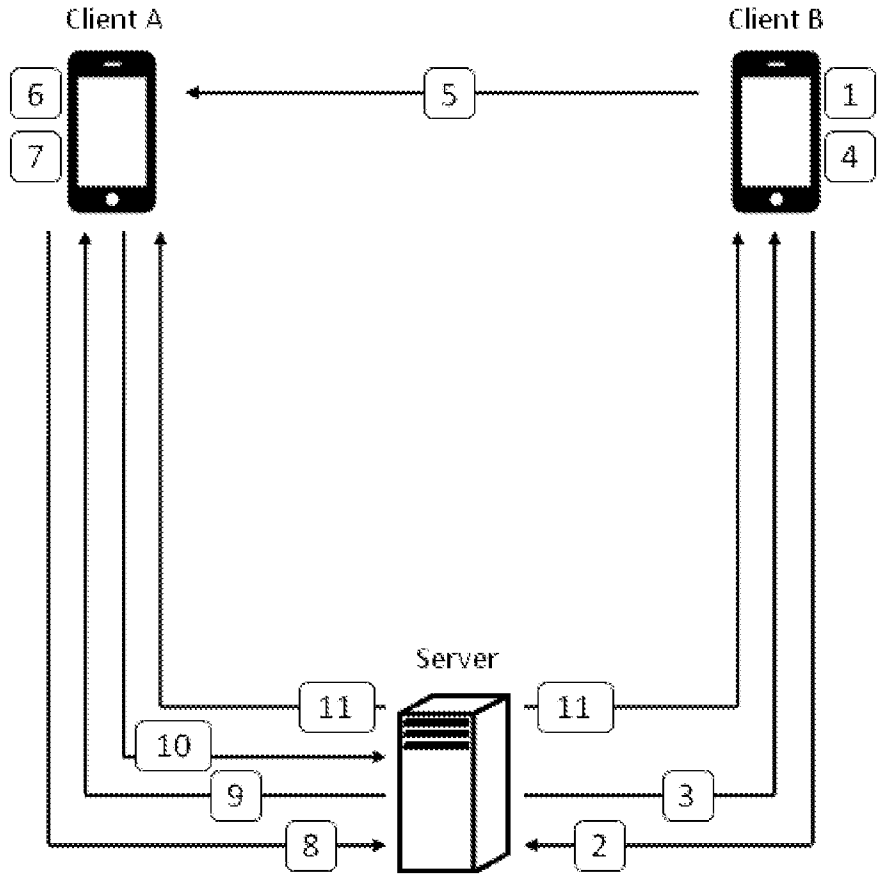


FIG. 15

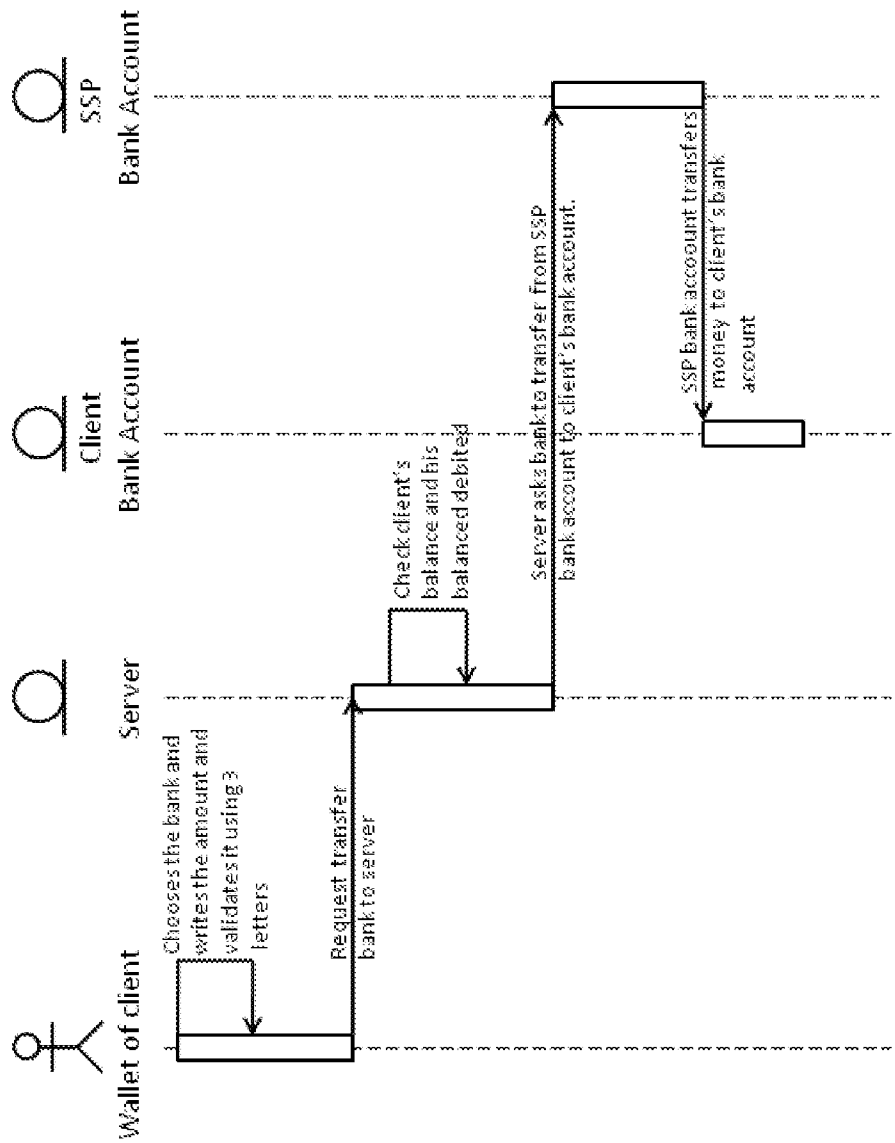

Wallet of client
Server
Client Bank Account
SSP Bank Account
Chooses the bank and writes the amount and validates it using 3 letters
Request transfer bank to server
Check client's balance and his balanced debited
Server asks bank to transfer from SSP bank account to client's bank account.
SSP bank account transfers money to client's bank account

FIG. 16

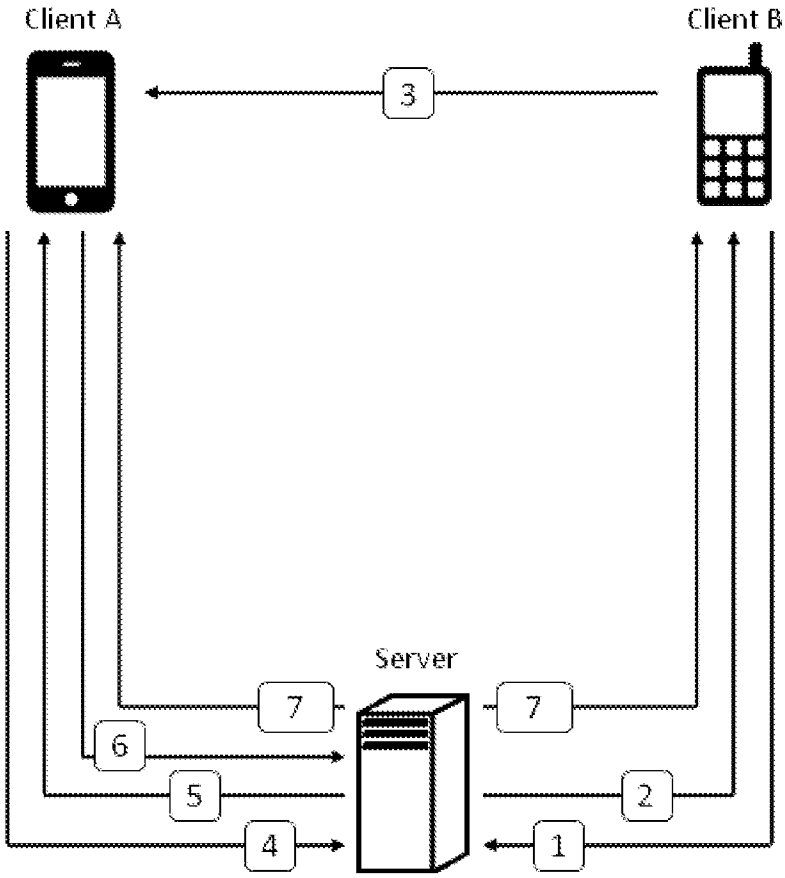


FIG. 17

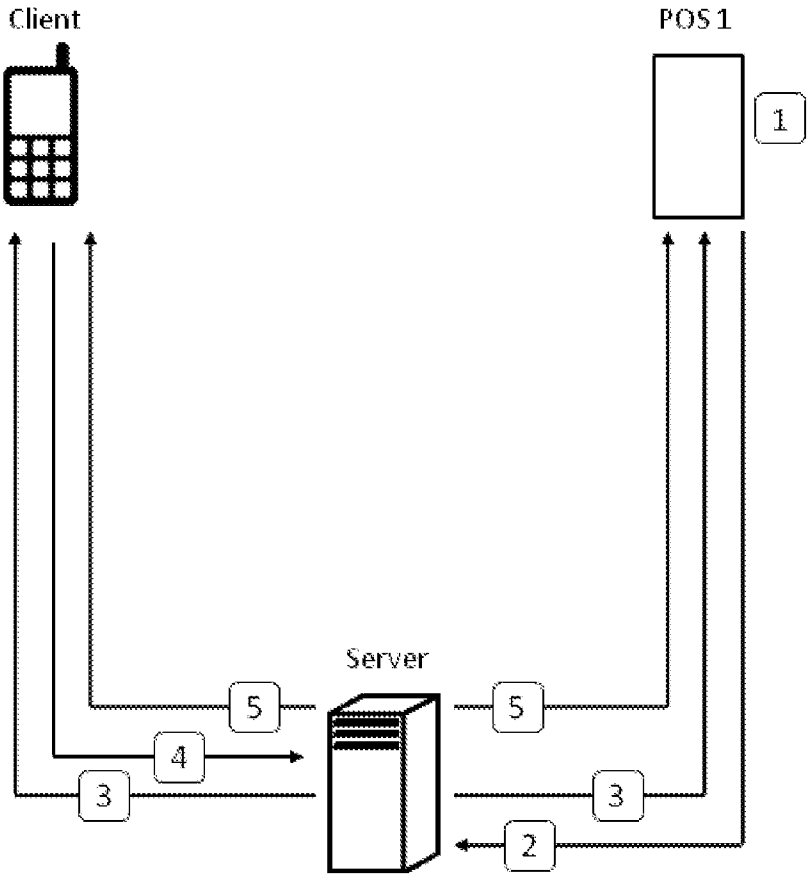


FIG. 18

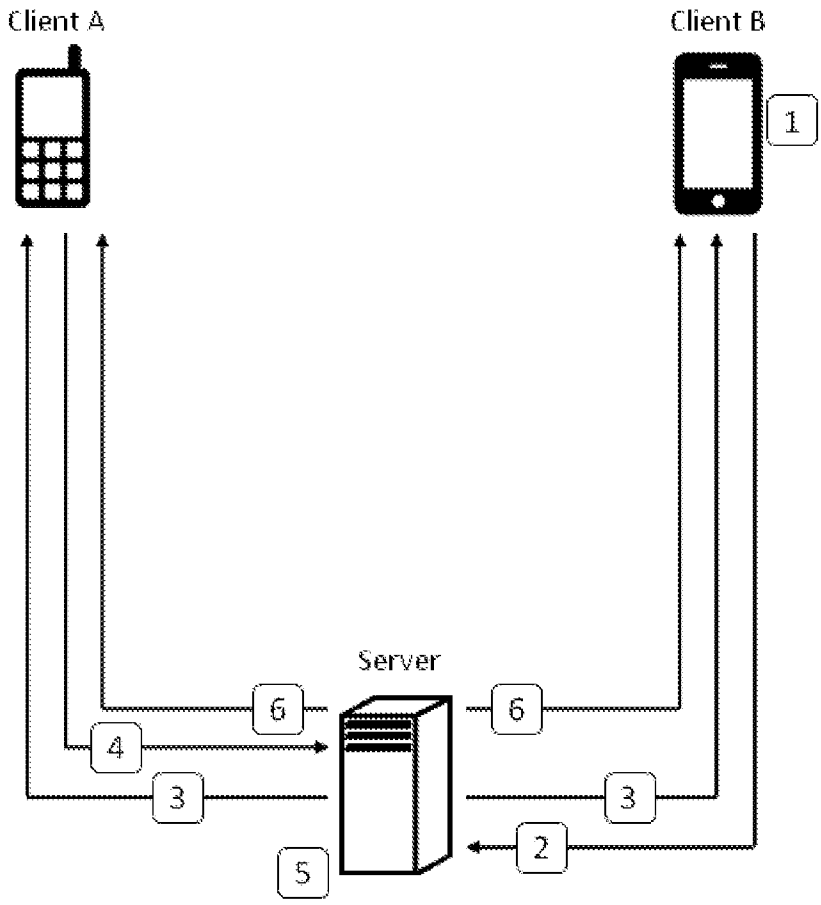


FIG. 19

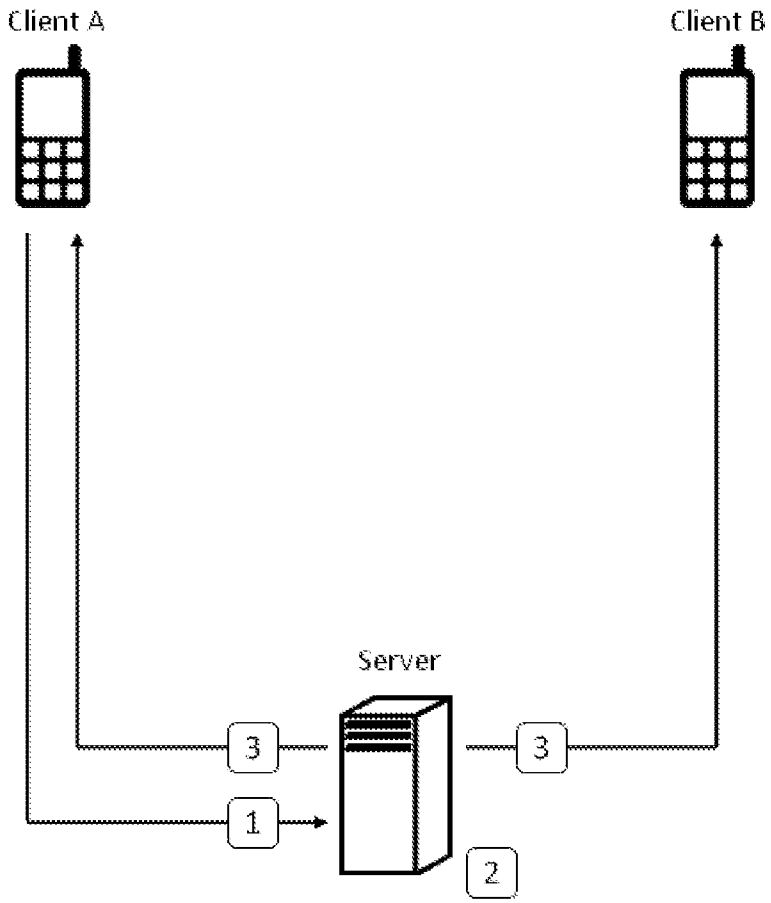


FIG. 20

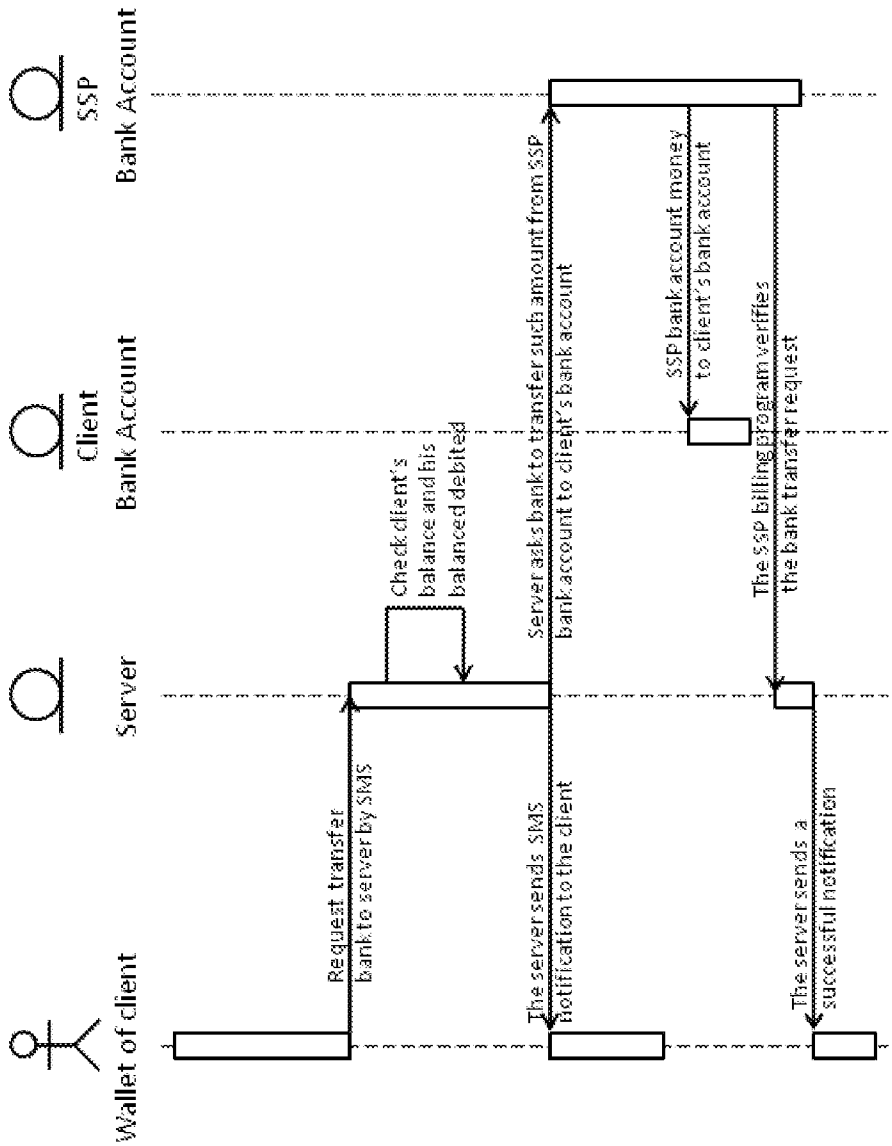

Wallet of client
Server
Client Bank Account
SSP Bank Account
Request transfer bank to server by SMS
Check client's balance and his balanced debited
Server asks bank to transfer such amount from SSP bank account to client's bank account
SSP bank account money to client's bank account
The SSP billing program verifies the bank transfer request
The server sends SMS notification to the client
The server sends a successful notification

FIG. 21

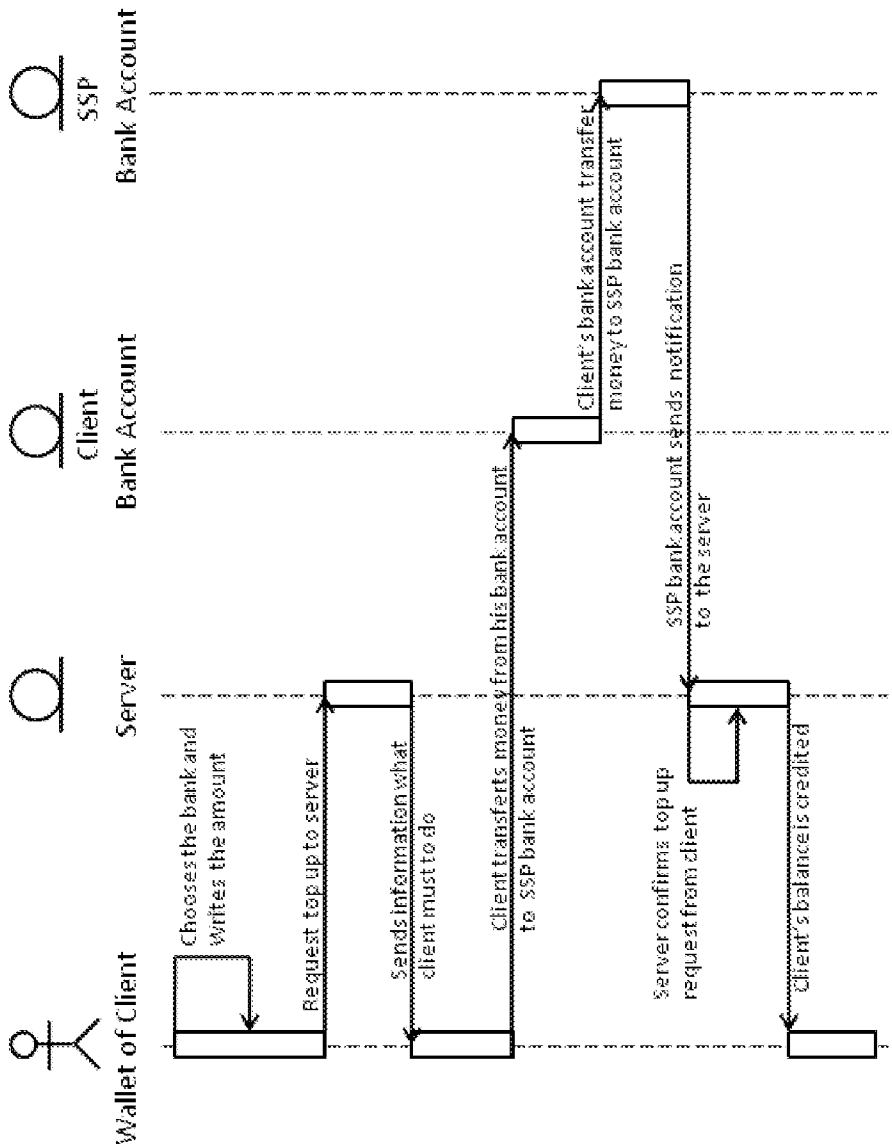

Wallet of Client
Server
Client Bank Account
SSP Bank Account
Chooses the bank and writes the amount
Request top up to server
Sends information what client must to do
Client transferts money from his bank account to SSP bank account
Client's bank account transfers money to SSP bank account
SSP bank account sends notification to the server
Server confirms top up request from client
Client's balance is credited

FIG. 22

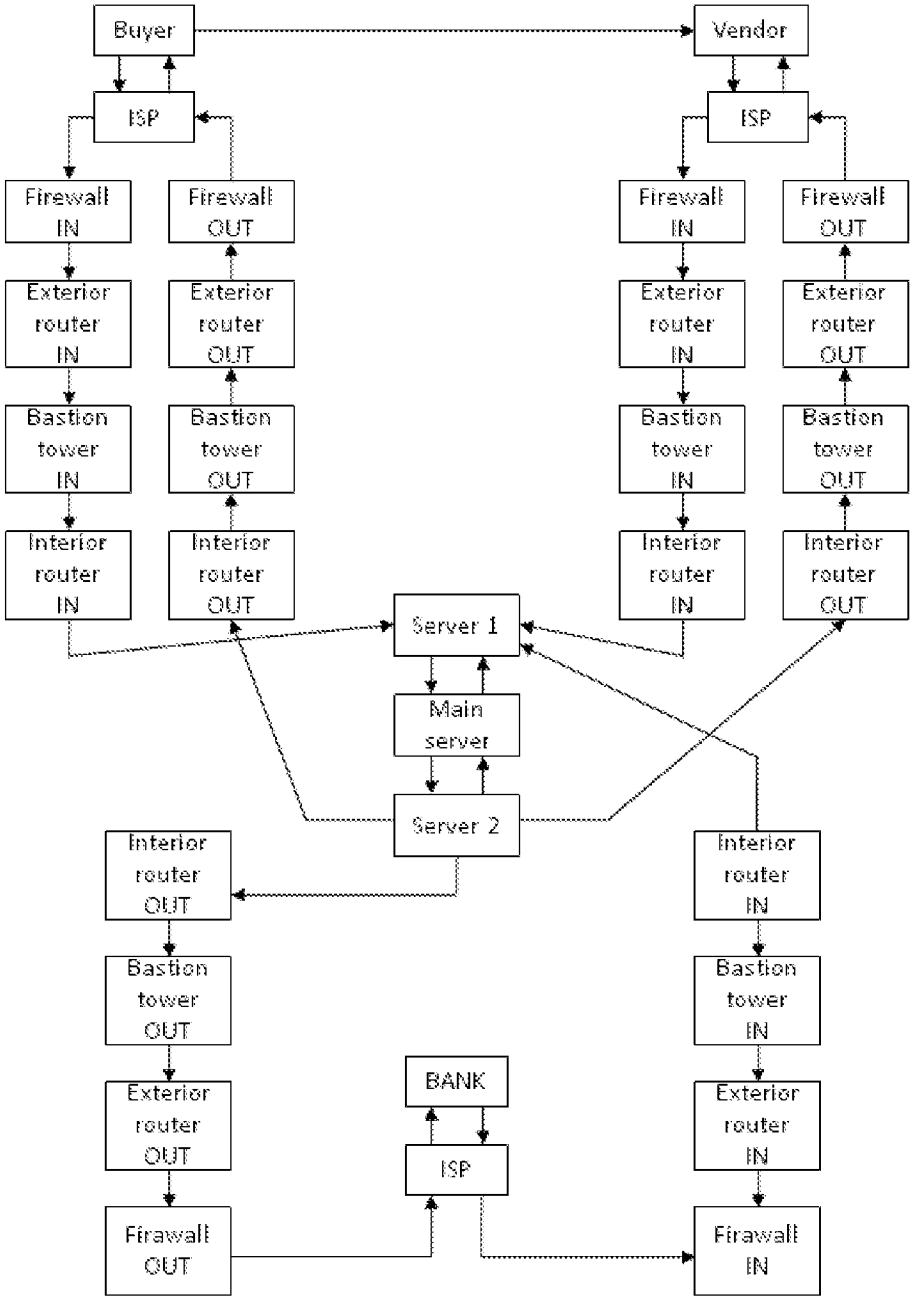

Buyer
Vendor
ISP
ISP
Firewall IN
Firewall OUT
Firewall IN
Firewall OUT
Exterior router IN
Exterior router OUT
Exterior router IN
Exterior router OUT
Bastion tower IN
Bastion tower OUT
Bastion tower IN
Bastion tower OUT
Interior router IN
Interior router OUT
Interior router IN
Interior router OUT
Server 1
Main server
Server 2
Interior router OUT
Interior router IN
Bastion tower OUT
Bastion tower IN
BANK
ISP
Exterior router OUT
Exterior router IN
Firawall OUT
Firawall IN

FIG. 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2016/052857

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/08 (2012.01) G06Q 20/32 (2012.01) G06Q 20/36 (2012.01) G06Q 30/06 (2012.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

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

EPODOC, WPIAP keywords: Transaction, Payment, Purchase, Buy, Money, Transfer, Real Time, Money, Cash, Fund, Fee, Credit, Transfer, Mobile, Tablet, Smartphone, PDA, Notebook, Electronic, Digital, Wallet and similar terms; **Google Patents/Freepatentsonline keywords:** Transaction, Payment, Transfer, Purchase, Buy, Mobile, Phone, Tablet, Smartphone, PDA, Notebook, Money, Cash, Fund, Fee, Credit, Wallet, Server, Hub, Merchant, Vendor, Store, Unidirectional, One Way, Plurality, User, Subscriber, Consumer, Customer, Payer, Recipient, Payee, Real Time, Virtual, Keyboard, Secure, Safe, Protect, Bank, Union, Account, NFC, QR, SMS, Text, Asymmetric, Path, Channel, Parallel and similar terms; **Google Patents/Espacenet/Auspat/Internal AU Databases:** *Applicant/Inventor: Downer; Prabowo, Febrianto, Febriyantoro, Lee Balada, Ainul Yaqin, Firdaus*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[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 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 September 2016	28 September 2016
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Evan Sules AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0399359617

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation).	DOCUMENTS CONSIDERED TO BE RELEVANT	**PCT/IB2016/052857**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2013/0332347 A1 (LIBERTY) 12 December 2013	
X	abstract, page 1, paragraphs 0003-0005; page 3, paragraph 0050; pages 3-4, paragraph 0051; page 4, paragraphs 0054, 0059; page 6, paragraphs 0076, 0083, 0086, 0087; pages 6-7, paragraph 0089; page 7, paragraphs 0090, 0094, 0096; page 8, paragraphs 0100, 0101; page 9, paragraph 0112 - page 10, paragraph 0117; pages 10-11, paragraph 0123; page 13, paragraph 0143 - page 14, paragraph 0151	1-5, 7-21, 26, 29, 30, 32-47, 50, 58, 61-67, 69-71
Y	page 6, paragraph 0087	52
A	As Above	6, 22-25, 27, 28, 31, 48, 49, 51, 53-57, 59, 60, 68
	US 2013/0282588 A1 (HRUSKA) 24 October 2013	
X	page 1, paragraphs 0003-0005; page 2, paragraph 0013 - page 3, paragraph 0018; pages 3-4, paragraph 0019	1-5, 7-18, 20, 22-26, 28-36, 48, 49, 51, 53-69
Y	As above	52
A	As above	6, 19, 21, 27, 37-47, 50, 70, 71
	US 2012/0209749 A1 (HAMMAD ET AL) 16 August 2012	
X	abstract; figure 2E; page 1, paragraph 0021 - page 2, paragraph 0026; page 7, paragraph 0045; page 11, paragraph 0061	1-5, 7-10, 12-21, 29, 30, 32-37, 40, 41, 50, 58
A	As above	6, 11, 22-28, 31, 38, 39, 42-49, 51-57, 59-71
	US 2009/0281904 A1 (PHARRIS) 12 November 2009	
X	page 1, paragraph 0010 - page 2, paragraph 0012; page 3, paragraphs 0029, 0030-0032; page 4, paragraph 0040; pages 4-5, paragraph 0041; page 5, paragraph 0048; page 6, paragraphs 0055, 0058; page 7, paragraph 0065 - page 9, paragraph 0082	1-10, 12-18, 20, 27-36, 45-47, 49, 53, 54, 56-58
Y	As above	52
A	As above	11, 19, 21-26, 37-44, 48, 50, 51, 55, 59-71
	US 2007/0255662 A1 (TUMMINARO) 01 November 2007	
X	page 4, paragraphs 0040, 0042; page 5, paragraphs 0045, 0047; page 8, paragraphs 0150, 0154; page 10, paragraph 0180; page 11, paragraphs 0189, 0199, 202; page 12, paragraph 0210 - page 13, paragraph 0219; page 14, paragraph 0234; page 35, paragraph 0467; page 37, paragraph 0518	1-5, 7-18, 20, 26, 29, 30, 32-47, 50, 58, 62, 63, 66, 67, 69-71
Y	As above	52
A	As above	6, 19, 21-25, 27, 28, 31, 48, 49, 51, 53-57, 59-61, 64, 65, 68

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2013/0332347 A1	12 December 2013	US 2013332347 A1	12 Dec 2013
		EP 2715632 A1	09 Apr 2014
		EP 2721562 A1	23 Apr 2014
		MX 2013014209 A	12 Jan 2015
		MX 2013015355 A	14 May 2014
		RU 2013158871 A	20 Jul 2015
		RU 2014101498 A	27 Jul 2015
		US 2012310824 A1	06 Dec 2012
		US 8538845 B2	17 Sep 2013
		US 2012323777 A1	20 Dec 2012
		US 2012330737 A1	27 Dec 2012
		US 2013246141 A1	19 Sep 2013
		US 2014006048 A1	02 Jan 2014
		US 2014201070 A1	17 Jul 2014
		US 2016055583 A1	25 Feb 2016
		WO 2013009444 A1	17 Jan 2013
		WO 2013009446 A1	17 Jan 2013
		WO 2013025273 A1	21 Feb 2013
		WO 2013166174 A1	07 Nov 2013
		WO 2016073519 A1	12 May 2016
US 2013/0282588 A1	24 October 2013	US 2013282588 A1	24 Oct 2013
US 2012/0209749 A1	16 August 2012	US 2012209749 A1	16 Aug 2012
		AU 2011316955 A1	30 May 2013
		AU 2012205511 A1	18 Jul 2013
		AU 2012217606 A1	09 May 2013
		AU 2012220669 A1	02 May 2013
		AU 2012278963 A1	23 Jan 2014
		AU 2013214801 A1	25 Sep 2014
		AU 2013277083 A1	22 Jan 2015
		AU 2014232707 A1	05 Nov 2015
		AU 2016203811 A1	30 Jun 2016
		AU 2016204018 A1	07 Jul 2016
		CN 103635920 A	12 Mar 2014
		CN 103765453 A	30 Apr 2014
		CN 105144216 A	09 Dec 2015

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		EP 2678812 A1	01 Jan 2014
		EP 2810242 A1	10 Dec 2014
		EP 2973276 A1	20 Jan 2016
		HK 1213076 A1	24 Jun 2016
		JP 2016524198 A	12 Aug 2016
		SG 193481 A1	30 Oct 2013
		SG 193510 A1	30 Oct 2013
		SG 11201404555W A	28 Aug 2014
		US 2012215648 A1	23 Aug 2012
		US 8571937 B2	29 Oct 2013
		US 2013121633 A1	16 May 2013
		US 8849075 B2	30 Sep 2014
		US 2013246261 A1	19 Sep 2013
		US 9355393 B2	31 May 2016
		US 2012123924 A1	17 May 2012
		US 2012124496 A1	17 May 2012
		US 2012209677 A1	16 Aug 2012
		US 2012215701 A1	23 Aug 2012
		US 2012233073 A1	13 Sep 2012
		US 2012239556 A1	20 Sep 2012
		US 2013013499 A1	10 Jan 2013
		US 2013024364 A1	24 Jan 2013
		US 2013024371 A1	24 Jan 2013
		US 2013054454 A1	28 Feb 2013
		US 2013151417 A1	13 Jun 2013
		US 2013159081 A1	20 Jun 2013
		US 2013159154 A1	20 Jun 2013
		US 2013166332 A1	27 Jun 2013
		US 2013204886 A1	08 Aug 2013
		US 2013204894 A1	08 Aug 2013
		US 2013218657 A1	22 Aug 2013
		US 2013246215 A1	19 Sep 2013
		US 2013246342 A1	19 Sep 2013
		US 2013290203 A1	31 Oct 2013
		US 2013290234 A1	31 Oct 2013
		US 2014019352 A1	16 Jan 2014

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		US 2014052617 A1	20 Feb 2014
		US 2014197234 A1	17 Jul 2014
		US 2014213344 A1	31 Jul 2014
		US 2014214653 A1	31 Jul 2014
		US 2014222594 A1	07 Aug 2014
		US 2014249999 A1	04 Sep 2014
		US 2014337175 A1	13 Nov 2014
		US 2015019944 A1	15 Jan 2015
		US 2015026049 A1	22 Jan 2015
		US 2015039462 A1	05 Feb 2015
		US 2015046241 A1	12 Feb 2015
		US 2015058162 A1	26 Feb 2015
		US 2015154588 A1	04 Jun 2015
		US 2015220914 A1	06 Aug 2015
		US 2015248664 A1	03 Sep 2015
		US 2016063486 A1	03 Mar 2016
		US 2016232513 A1	11 Aug 2016
		WO 2012054785 A1	26 Apr 2012
		WO 2012054786 A1	26 Apr 2012
		WO 2012097108 A1	19 Jul 2012
		WO 2012112822 A2	23 Aug 2012
		WO 2012116125 A1	30 Aug 2012
		WO 2013006725 A2	10 Jan 2013
		WO 2013009660 A1	17 Jan 2013
		WO 2013012876 A1	24 Jan 2013
		WO 2013044175 A1	28 Mar 2013
		WO 2013049329 A1	04 Apr 2013
		WO 2013075071 A1	23 May 2013
		WO 2013090611 A2	20 Jun 2013
		WO 2013116806 A1	08 Aug 2013
		WO 2013192443 A1	27 Dec 2013
		WO 2014011691 A1	16 Jan 2014
		WO 2014145708 A1	18 Sep 2014

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2009/0281904 A1	12 November 2009	US 2009281904 A1	12 Nov 2009
		AR 084339 A1	08 May 2013
		AU 2009251572 A1	03 Dec 2009
		AU 2009251576 A1	03 Dec 2009
		AU 2009251577 A1	03 Dec 2009
		BR PI0911093 A2	06 Oct 2015
		BR PI0911095 A2	06 Oct 2015
		BR PI0911097 A2	06 Oct 2015
		CA 2719944 A1	03 Dec 2009
		CA 2719945 A1	03 Dec 2009
		CA 2720126 A1	03 Dec 2009
		CN 101990676 A	23 Mar 2011
		CN 101990770 A	23 Mar 2011
		CN 101990772 A	23 Mar 2011
		CO 6311124 A2	22 Aug 2011
		CO 6311125 A2	22 Aug 2011
		DO P2010000288 A	15 Mar 2011
		DO P2010000289 A	15 Mar 2011
		EA 201071154 A1	30 Jun 2011
		EA 201071155 A1	30 Jun 2011
		EA 201071156 A1	30 Jun 2011
		EC SP10010590 A	28 Feb 2011
		EC SP10010591 A	28 Feb 2011
		EP 2266087 A2	29 Dec 2010
		EP 2266332 A1	29 Dec 2010
		EP 2266335 A1	29 Dec 2010
		JP 2011516980 A	26 May 2011
		JP 2011518377 A	23 Jun 2011
		KR 20100123895 A	25 Nov 2010
		KR 20100123896 A	25 Nov 2010
		KR 20100135249 A	24 Dec 2010
		MX 2010010810 A	21 Dec 2010
		MX 2010010811 A	20 Dec 2010
		MX 2010010812 A	20 Dec 2010
		NZ 588573 A	25 May 2012

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		TW 201005667 A	01 Feb 2010
		TW 201241766 A	16 Oct 2012
		US 2009254440 A1	08 Oct 2009
		US 8301500 B2	30 Oct 2012
		US 2009254479 A1	08 Oct 2009
		US 2012047070 A1	23 Feb 2012
		WO 2009146106 A1	03 Dec 2009
		WO 2009146110 A1	03 Dec 2009
		WO 2009146111 A2	03 Dec 2009
		WO 2012082899 A1	21 Jun 2012

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2007/0255662 A1	01 November 2007	US 2007255662 A1	01 Nov 2007
		BR PI0710021 A2	02 Aug 2011
		BR PI0710089 A2	23 Aug 2011
		CA 2647602 A1	06 Mar 2008
		CA 2647636 A1	06 Mar 2008
		CN 101454794 A	10 Jun 2009
		CN 101454795 A	10 Jun 2009
		EP 2008237 A1	31 Dec 2008
		EP 2013842 A1	14 Jan 2009
		EP 2266083 A2	29 Dec 2010
		EP 2304678 A1	06 Apr 2011
		EP 2344994 A1	20 Jul 2011
		EP 2407918 A1	18 Jan 2012
		EP 2407919 A1	18 Jan 2012
		MX 2008012503 A	12 Dec 2008
		MX 2008012504 A	05 May 2009
		US 2009119190 A1	07 May 2009
		US 7873573 B2	18 Jan 2011
		US 2007233615 A1	04 Oct 2007
		US 8249965 B2	21 Aug 2012
		US 2007230371 A1	04 Oct 2007
		US 8532021 B2	10 Sep 2013
		US 2007244811 A1	18 Oct 2007
		US 2007255620 A1	01 Nov 2007
		US 2007255652 A1	01 Nov 2007
		US 2007255653 A1	01 Nov 2007
		US 2008032741 A1	07 Feb 2008
		US 2009287601 A1	19 Nov 2009
		US 2009319425 A1	24 Dec 2009
		US 2010063935 A1	11 Mar 2010
		US 2011320347 A1	29 Dec 2011
		WO 2008027620 A1	06 Mar 2008
		WO 2008027621 A1	06 Mar 2008
		WO 2009114876 A2	17 Sep 2009
		WO 2009152184 A1	17 Dec 2009

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2016/052857**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		WO 2010082960 A1	22 Jul 2010
		WO 2011163525 A1	29 Dec 2011

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.