(51) International Patent Classification:
G06Q 20/32 (2012.01)  G07F 19/00 (2006.01)
G06Q 20/02 (2012.01)

(21) International Application Number:
PCT/IB20 13/000 144

(22) International Filing Date:
4 February 2013 (04.02.2013)

(25) Filing Language: English

(26) Publication Language: English

(72) Inventor: and

(74) Agent: KESCHMANN, Mare; Haffher und Keschnann, Patentanwalte KG, Schottengasse 3a, A-1014 Vienna (AT).


(54) Title: METHOD AND SYSTEM FOR PERFORMING A FINANCIAL TRANSACTION

(57) Abstract: In a method of performing a financial transaction, a payment processing server having merchant accounts and client accounts stored therein is provided, wherein said accounts each comprise an account ID and data regarding a financial account held on a financial institution, a processing request is received from a merchant, a transaction session is started, wherein said transaction data comprises creating and storing, in the payment processing server, a unique transaction code, the transaction code is transmitted to a merchant device, from the merchant device to a client's mobile telecommunication device, and from the mobile device to the payment processing server, a clearing request message is sent from the payment processing server to the financial institution of the client's and/or the merchant's financial account, and, after a clearing response message is received, a transfer of the transaction amount from the client's financial account to the merchant's financial account is caused.
The invention refers to a method and a system for performing a financial transaction and to a method of operating a payment processing server for performing financial transactions.

Further, the invention refers to a computer program product that comprises program code which, when loaded into a computer, carries out the inventive method.

A great variety of methods and systems for performing financial transactions have already been proposed that allow clients (customers) to perform financial transactions by simply using their mobile telecommunication device. The term "digital wallet" is also increasingly being used to describe mobile phones, especially smartphones, that store an individual's credentials and utilize wireless technologies such as near field communication (NFC) to carry out financial transactions.

An individual's bank account is usually linked to the digital wallet. The credentials can be passed to a merchant's terminal wirelessly via NFC. Typically, digital wallets are stored on the client side and are easily self-maintained. A server-side digital wallet is one that an organization creates for and about users and maintains on its servers. Server-side digital wallets are gaining popularity due to the security, efficiency, and added utility it provides to the end-user. The information component is basically a database of user-inputted information. This information consists of shipping address, billing address, payment methods (including credit card numbers, expiry dates, and security numbers), and other information.
Most of the known systems, such as digital wallets, require the transmission of personal data, such as credit card numbers or e-wallet user account data, to the merchant. In these systems a certain degree of security is offered by providing encrypted transmission of the personal information and encryption for the actual transaction. However, the drawback of such systems is that only the transmission channel is secure so that the merchant may still be able to read and possibly misuse the confidential personal information provided by the client. In systems that are designed to pass the personal information through the merchant's system without being decrypted, the merchant or any fraudulent third party braking into the merchant's system might still be able to successfully brake the encryption.

On the other hand, there are also systems that allow the client's mobile device to connect to an e-commerce data center operated by the merchant for directly retrieving transaction related data, such as billing data. This involves the risk of unauthorized parties entering the merchant's data center and either stealing or manipulating confidential data for fraudulent purposes.

Therefore, the invention aims at overcoming the above drawbacks and security issues and at providing an easy and secure transaction method wherein neither the client nor the merchant have to transmit confidential or personal information to the other party. A further object of the invention is to provide a payment system that is not bound to a specific predetermined payment method, but that is capable of managing various payment methods (such as, e.g., bank accounts, credit cards, cash vouchers, PayPal accounts, etc.).
To solve the above object, the invention provides a method of performing a financial transaction, comprising:

- providing a payment processing server having merchant accounts and client accounts stored therein, wherein said accounts each comprise an account ID and data regarding a financial account held at a financial institution,
- receiving, in the payment processing server, a processing request from a merchant, the processing request including a merchant account ID and transaction-related information including at least a transaction amount,
- starting, in the payment processing server, a transaction session, wherein said transaction session comprises creating and storing, in the payment processing server, a unique transaction code,
- transmitting the transaction code to a merchant device,
- transmitting the transaction code from a merchant device to a client's mobile telecommunication device, the mobile telecommunication device having a client account ID stored therein,
- transmitting the transaction code together with the client account ID from the client's mobile telecommunication device over a telecommunication network to the payment processing server,
- obtaining, in the client's mobile telecommunication device, the transaction amount and optionally other transaction details (like quantity, merchant order ID) from the payment processing server and displaying the transaction amount,
- authorizing, by the client, the transaction amount and transmitting an authorization message to the payment processing server,
- sending a clearing request message from the payment processing server to the financial institution of the client's and/or the merchant's financial account,
- receiving, in the payment processing server, a clearing response message,
- if the clearing response message is positive, causing a transfer of the transaction amount from the client's financial account to the merchant's financial account.

Further, the invention provides a method of operating a payment processing server for performing financial transactions, comprising
- keeping merchant accounts and client accounts on the payment processing server, wherein said accounts each comprise an account ID and data regarding a financial account held at a financial institution,
- receiving, in the payment processing server, a processing request from a merchant, the processing request including a merchant account ID and transaction-related information including at least a transaction amount,
- starting, in the payment processing server, a transaction session, wherein said transaction session comprises creating and storing, in the payment processing server, a unique transaction code,
- transmitting the transaction code to a merchant device,
- receiving, in the payment processing server, the transaction code together with a client account ID from a client's mobile telecommunication device over a telecommunication network,
- transmitting the transaction amount from the payment processing server to the client's mobile telecommunication device,
receiving, in the payment processing server, an authorization message from the client's mobile telecommunication device,
- sending a clearing request message from the payment processing server to the financial institution of the client's and/or the merchant's financial account,
- receiving, in the payment processing server, a clearing response message,
- if the clearing response message is positive, causing a transfer of the transaction amount from the client's financial account to the merchant's financial account.

According to a preferred embodiment, the processing request may be sent from the merchant device to the payment processing server.

Thus, instead of transmitting personal data, such as bank account numbers or credit card numbers from the client to the merchant, the invention provides for the transmission of a transaction code from the merchant to the client. The transaction code allows the client to retrieve an electronic bill from the payment processing server and to authorize the payment through the payment processing server. Compared to most existing payment systems the invention provides for an inversion of the information flow, namely from the merchant to the client instead of from the client to the merchant. Apart from the transmission of the transaction code, which preferably neither contains personal information nor transaction-related information, both, the merchant and the client exchange their information exclusively with the payment processing server. The payment processing server is the only instance that knows both, the data of the merchant and of the client, i.e. the issuing and the acquiring payment data. No client data is exchanged
with the merchant or any other intermediaries in the communication chain thereafter. In this way, client's personal data is protected against misuse by the merchant or any other third party and merchant's data (such as transaction related data, financial account data) is protected against fraud and the merchant is protected against faked client data.

The transaction code is a unique code that identifies the transaction session started in the payment processing server. The transaction code may be a random code. Preferably, the transaction code does not comprise any coded transaction related data, such as billing data. Preferably, the transaction code does not comprise any coded personal data neither from the client nor from the merchant.

The merchant accounts and the client accounts held in the payment processing server each comprise an account ID, which serves to identify the respective account. The account ID is a unique identifier and is attached by the merchant device and the client's mobile telecommunication device, respectively, to any data transmitted to the payment processing server in order to enable the payment processing server to assign the transmitted data to the correct account. The client account ID may preferably be a unique identifier of the client's mobile telecommunication device, such as the IMEI of client's mobile phone or the mobile phone number. The merchant account ID may preferably also be a unique merchant device identifier.

The merchant account and the client account held with the payment processing server may comprise additional information, such as personal data like name, address and date of birth, as well as a photo. Further, the account comprises data regarding a financial account held at a financial institution. The
financial account may be a bank account, a credit/debit card or an e-Wallet account, such as a PayPal account. However, within the context of the invention, the financial institution must not necessarily be a bank. Rather, the financial account may also relate to cash vouchers or to direct mobile operator billing. Preferably, the financial institution account assigned the merchant is an acquiring bank, i.e. a payment system that transacts to receive money from an issuing bank. Correspondingly, the financial institution account assigned to the client preferably is an issuing bank, i.e. a payment system that push money to the acquiring bank. Rope Pay is a mobile payment system agnostic of payment methods. Various payment methods can be added, e.g. direct bank account debit (EPS), credit/debit cards, cash vouchers, direct mobile operator billing, etc. Preferably, the payment processing server itself does not act as an acquirer, but only clears the transaction with an external acquirer. The clearing of the transaction preferably comprises the following steps:
- sending a clearing request message from the payment processing server to the merchant's acquirer,
- receiving, in the payment processing server, a clearing response message from the merchant's acquirer.

Because the payment processing system preferably does not act as an acquirer, the payment processing server primarily functions as a gateway on top of a variety of payment methods and also allows functioning as a bridge between different issuing and acquiring payment methods (e.g. from credit card to cash voucher).

A client account held at the payment processing server may comprise data regarding a plurality of financial accounts. In this case, the client may at each transaction choose the
Every client and merchant needs to register with the payment processing server. Personal data like name, address and date of birth, as well as optionally a photo (using the phone's built in camera) are sent to the payment processing server, which creates the account. Depending on the account type (client, merchant) and country's regulations, further KYC (Know Your Customer) procedures might be necessary until the account becomes fully operational. In connection with the registration process, the payment processing server may preferably collect some data about the merchant device or the client's mobile telecommunication device, such as the IMEI or a hardware fingerprint. All collected data is sent to the payment processing server. By collecting data about the merchant device or the client's mobile telecommunication device it is possible to bind the respective device to the user's account, so that the user can use the payment processing server's services only when using a registered device. The payment processing server may, however, allow a client to register several mobile devices and attach all of them to the same client account.

The communication between the merchant device or the client's mobile telecommunication device on the one side and the payment processing server on the other side may preferably be performed over a secure communication channel. Preferably, the secure channel is established by using public-key cryptography. Thus all data is encrypted/decrypted by using a public key. The creation of a key pair consisting of a private key and a public key for use in the public-key cryptography may preferably be done in the payment processing server. The payment processing server may then send the public key to the merchant device or
the client's mobile telecommunication device, respectively. This public key is used to encrypt the communication with the payment processing server. The payment processing server preferably creates the key pair on basis of the IMEI and/or the hardware fingerprint received from the respective device (merchant device or client's mobile telecommunication device). In this way, the server side client/merchant account is bound to the user's device. There is no data stored on the merchant device and on the client device, apart from the public key. During registration the client may preferably choose a personal PIN code, which is used as a passphrase to secure the local key.

The preferred way of communication between the user's device (i.e. the merchant device or the client's mobile telecommunication device) is via a data connection, such as via Wireless LAN or via a data communication protocol described in the GSM standard. If compatible with the data communication protocol, an SSL connection can be used. The transmission of any data is thus double encrypted: once by the SSL channel, and once by the public key encryption itself, within the SSL. In case a data connection is not available, SMS (Short Message Service) and USSD (Unstructured Supplementary Service Data) may also be used as communication channels. In this case the public key encrypted data can preferably be transported as PDU (protocol data unit) messages.

Within the context of the invention, a payment processing server may be a computer hardware system, such as a backend data center, dedicated to run one or more services as a host to process transactions. In particular, such a server is able to handle multiple transaction sessions at a time and to send and
receive data to and from the merchant device and the client's mobile telecommunication device.

In order to efficiently use the computing power of at least the client's mobile device, the client-side and optionally the merchant-side functions required to perform the inventive method are implemented in a program application installed on the merchant device or the client's mobile telecommunication device, respectively.

The client's mobile telecommunication device may preferably be any form of mobile computer having a display, such as a mobile phone, a smart phone, a tablet computer etc.

The merchant device may preferably be a mobile device having a display, such as a mobile phone, a smart phone, a tablet computer etc., a printed bill, an e-commerce web server together with a client computer connected to the server, or a POS device having an electronic display. In the case of a printed bill the step of transmitting the transaction code to a merchant device comprises printing the transaction code onto a carrier, such as paper. The transaction code may also be printed or shown on billboards or on TV and Satellite channels. The client may then transfer the transaction code to his mobile telecommunication device manually or by optical sensing means. In the case of the merchant using an eCommerce web system, the transaction code may preferably be transmitted to the eCommerce web server and displayed to the client on a client computer via a web page generated by the eCommerce web server. An API may preferably be integrated into the merchant's eCommerce systems in order to facilitate the communication with the payment processing server.
The transaction code may be transferred or transmitted from the merchant device to the client's mobile telecommunication device in any possible way. In one embodiment, the transmission of the transaction code comprises presenting the transaction code as a graphical code on the merchant device and reading the graphical code by means of an optical sensor of the client's mobile telecommunication device. The optical sensor may preferably be a photo camera of the mobile device. The graphical code may be a QR code, which is handy because of its high error tolerance. Alternatively, standard 2D codes, bar codes, or any other information that can be decoded from an image can also be used. The encoding of the transaction code is preferably done in the payment processing server.

Alternatively, the transaction code may be transmitted from the merchant device to the client's mobile telecommunication device by wireless electronic near-field communication, such as, e.g., radio communication or capacitive coupling, in particular NFC and similar RFID techniques.

Alternatively or in addition, the transaction code may be transmitted by presenting the transaction code as an alphanumerical code on the merchant device and manually entering the alphanumerical code into the client's mobile telecommunication device. This embodiment is particularly suitable for allowing the use of mobile devices by the client that do not have the capability of capturing an image or of receiving wireless electronic near-field communication.

According to a preferred embodiment the transaction session comprises
- creating and storing, in the payment processing server, a transaction dataset comprising the transaction-related
information and assigning the transaction dataset to the merchant account having the merchant account ID received together with the processing request,

- assigning the transaction code to the transaction dataset,
- in the payment processing server, matching the transaction code received from the client's mobile telecommunication device with stored transaction codes, identifying the transaction dataset to which the matching transaction code is assigned and assigning the transaction dataset to the client account having the client account ID received from the client's mobile telecommunication device.

According to a preferred embodiment, the step of authorizing the transaction amount comprises generating and displaying an authorization code input request on the client's mobile telecommunication device, and entering, by the client, an authorization code, into the mobile telecommunication device, and verifying the authorization code. The authorization code may be a PIN required by the client's financial institution in order to authorize access to the financial account. In particular, the authorization message transmitted to the payment processing server may comprise the authorization code and the authorization code is added to the clearing request message transmitted to the financial institution.

In the following, exemplary embodiments of the invention will be described in more detail with reference to the accompanying drawings. Fig. 1 shows an exemplary system diagram, in accordance with one embodiment of the invention.

With reference to Fig. 1, in a first step of the payment process, a merchant application is started on a merchant device 1. The merchant device 1 can be the merchant's mobile phone or
tablet, a display connected to a POS system at the merchant's site or an eCommerce site the client surfs on, e.g. at the payment screen of the merchant's shopping cart.

The merchant uses the merchant application (or the merchant's software uses a plugin & API) to create an electronic bill. For this purpose, he enters the transaction amount due and other bill data.

In the next step SI the application connects to the payment processing server 2 and transmits the bill data. Then, the payment processing server 2 starts a transaction session and creates a unique transaction code for this transaction and, in step S2, sends the transaction code together with a unique QR (quick response) code 3 that represents the transaction code back to the merchant device 1. Below the QR code image 3 the transaction code may also be displayed in clear text on the merchant device 1.

Subsequently, the client starts the client program application on his mobile phone 4. He uses the application to scan the QR Code 3 using the phone's built in camera in step S3. If the phone 4 does not have a built in camera, the clear text transaction code can be entered manually.

In step S4, the client application sends the transaction code to the payment processing server 2. The server 2 looks up the bill data and, in step S5 sends it back to the client application, which in turn displays it to the client. If the client chooses to continue with the payment, he can select the payment method and then enters his personal application PIN code to authorize the payment.
Alternatively, the PIN code may be used differently if needed. In case a financial institution (bank) demands that the client enters his personal bank PIN code or a TAN code, then the client application will require the client to enter this code instead of the personal application PIN for authorization. There are two methods of implementation: (i) OTA: the bank sends a SMS to the client with a mobile TAN (valid for several minutes), which must be entered manually into the client application for authorization; and (ii) if the payment processing server is allowed to connect to the bank by APIs, the client may enter his TAN into the client application directly.

In step S6 the client application sends an authorization message to the payment processing server, which, in turn clears the transaction between the Acquirer 5 and Issuer 6. The clearing involves sending a clearing request message from the payment processing server 2 to the Acquirer 5 in step S7 and receiving back a clearing response message in step S8. If the clearing response message is positive, a transfer of the transaction amount from the Issuer to the Acquirer is performed. Finally, in step S9 the result of the transaction in the form of a payment confirmation message is pushed simultaneously to both, the merchant device 1 and client's mobile phone 4.

The instant invention can be used for all kinds of financial transactions. Therefore, the term "merchant" does not limit the invention to transactions between a retail merchant and a consumer buying goods or services from the retail merchant. Rather, the term "merchant" generally refers to any receiver of money. Accordingly, the term "client" refers to any sender of money. For example, the invention can be used for cashing in or
cashing out money from a financial account associated with his client account held in the payment processing server.

This may preferably be accomplished with the help of mobile carrier agents, post offices and railway stations ("Agent"), that function as a "merchant". If a client wants to pay in cash or get cash out he visits an agent. He tells the agent about the type of transaction and the amount. The agent uses a merchant device as described above with reference to Fig. 1 running a merchant program application in exactly the same way as other merchants to create a bill. By configuration of the agent's merchant account, the payment processing server knows that this is a 'special' merchant. For cash out, the agent simply enters the desired amount. For cash-in transactions, a negative amount is entered, creating a credit note. After the transaction is complete, the cash money is exchanged between the parties.

As a further example, the invention may be used by a client for withdrawing money from his financial account associated with his client account held in the payment processing server. The transaction flow is similar to the agent cash-out described above and can be implemented for ATMs. The ATM's operator will function as the "merchant". The traditional way for a client is to put his credit card into the machine. The data on these cards has many times been faked or stolen. With the instant invention, the ATM cash withdrawal works as follows:

1. The client chooses to withdraw cash in accordance with the invention on the ATM screen and enters the desired amount
2. The ATM starts the transaction with the payment processing server and displays the transaction code (such as a QR code)
3. The scan by client and further flow of the transaction is the same as with a standard merchant transaction.

4. If the transaction is successful, the ATM will serve the cash.

5. If the ATM is also capable of receiving cash money, the same procedure can be applied with cash-in.

In a further exemplary embodiment of the invention, a geographical location function may preferably be implemented. Mobile phones with built in GPS functionality may be geo-located by the payment processing server. This can be used to implement security measures (payments from different locations during a short time span are suspicious, the merchant device and the client device must be in proximity, etc.), comfort (e.g. automatic recognition of a client when he enters a shop, for regular customers), and advertisements (e.g. special offers).

In a further exemplary embodiment of the invention, a "pay on delivery" function may preferably be implemented. This is a special, deferred payment method, especially tailored to home delivery businesses (eCommerce, pizza service, etc.). The actual payment is deferred until the parcel is delivered to the doorstep. This creates trust and eliminates fraud. In order to implement the "pay on delivery" function, the steps of the transaction method according to the invention and the sequence of these steps must not be changed in any way. The merchant starts the process as usual by sending a processing request to the payment processing server, whereafter a transaction session is started in the server and a transaction code is transmitted to the merchant. The merchant may preferably print a bill including the transaction code (such as a QR code) or print the transaction code (such as a QR code) on the parcel to be
delivered to the client. When delivering the parcel to the client, the client transmits the code to his client device (such as by scanning the QR code with the built-in camera of his mobile phone) and the transaction process proceeds in the usual way.
Claims:

1. A method of performing a financial transaction, comprising:

- providing a payment processing server having merchant accounts and client accounts stored therein, wherein said accounts each comprise an account ID and data regarding a financial account held at a financial institution,
- receiving, in the payment processing server, a processing request from a merchant, the processing request including a merchant account ID and transaction-related information including at least a transaction amount,
- starting, in the payment processing server, a transaction session, wherein said transaction session comprises creating and storing, in the payment processing server, a unique transaction code,
- transmitting the transaction code to a merchant device,
- transmitting the transaction code from a merchant device to a client's mobile telecommunication device, the mobile telecommunication device having a client account ID stored therein,
- transmitting the transaction code together with the client account ID from the client's mobile telecommunication device over a telecommunication network to the payment processing server,
- obtaining, in the client's mobile telecommunication device, the transaction amount from the payment processing server and displaying the transaction amount,
- authorizing, by the client, the transaction amount and transmitting an authorization message to the payment processing server,
- sending a clearing request message from the payment processing server to the financial institution of the client's and/or the merchant's financial account,
- receiving, in the payment processing server, a clearing response message,
- if the clearing response message is positive, causing a transfer of the transaction amount from the client's financial account to the merchant's financial account.

2. A method of operating a payment processing server for performing financial transactions, comprising
- keeping merchant accounts and client accounts on the payment processing server, wherein said accounts each comprise an account ID and data regarding a financial account held at a financial institution,
- receiving, in the payment processing server, a processing request from a merchant, the processing request including a merchant account ID and transaction-related information including at least a transaction amount,
- starting, in the payment processing server, a transaction session, wherein said transaction session comprises creating and storing, in the payment processing server, a unique transaction code,
- transmitting the transaction code to a merchant device,
- receiving, in the payment processing server, the transaction code together with a client account ID from a client's mobile telecommunication device over a telecommunication network,
- transmitting the transaction amount from the payment processing server to the client's mobile telecommunication device,
receiving, in the payment processing server, an authorization message from the client's mobile telecommunication device,

- sending a clearing request message from the payment processing server to the financial institution of the client's and/or the merchant's financial account,

- receiving, in the payment processing server, a clearing response message,

- if the clearing response message is positive, causing a transfer of the transaction amount from the client's financial account to the merchant's financial account.

3. A method according to claim 1 or 2, wherein said transaction session comprises

- creating and storing, in the payment processing server, a transaction dataset comprising the transaction-related information and assigning the transaction dataset to the merchant account having the merchant account ID received together with the processing request,

- assigning the transaction code to the transaction dataset,

- in the payment processing server, matching the transaction code received from the client's mobile telecommunication device with stored transaction codes, identifying the transaction dataset to which the matching transaction code is assigned and assigning the transaction dataset to the client account having the client account ID received from the client's mobile telecommunication device.

4. A method according to claim 1 or 2, wherein transmitting the transaction code from the merchant device to the client's mobile telecommunication device comprises presenting the transaction code as a graphical code on the merchant device and
reading the graphical code by means of an optical sensor of the
client's mobile telecommunication device.

5. A method according to claim 1 or 2, wherein the
transaction code is transmitted from the merchant device to the
client's mobile telecommunication device by wireless electronic
near-field communication, such as, e.g., radio communication or
capacitive coupling.

6. A method according to claim 1 or 2, wherein transmitting
the transaction code from the merchant device to the client's
mobile telecommunication device comprises presenting the
transaction code as an alphanumerical code on the merchant
device and manually entering the alphanumerical code into the
client's mobile telecommunication device.

7. A method according to any one of claims 1 to 6, wherein
the merchant device is selected from the group consisting of a
mobile telecommunication device having an electronic display, a
printed bill, an e-commerce web server together with a client
computer connected to the server, and a POS device having an
electronic display.

8. A method according to any one of claims 1 to 7, wherein
the step of authorizing the transaction amount comprises
generating and displaying an authorization code input request
on the client's mobile telecommunication device, and entering,
by the client, an authorization code, into the mobile
telecommunication device, and verifying the authorization code.

9. A method according to claim 8, wherein the authorization
message transmitted to the payment processing server comprises
the authorization code and the authorization code is added to
the clearing request message transmitted to the financial institution.

10. A method according to any one of claims 1 to 9, further comprising transmitting the clearing response message or a payment confirmation message from the payment processing server to the merchant device and/or to the client's mobile telecommunication device and displaying the message on said device(s).

11. A system for performing a financial transaction, comprising:
- a payment processing server having merchant accounts and client accounts stored therein, wherein said accounts each comprise an account ID and data regarding a financial account held at a financial institution,
- a client program application adapted to run on a mobile telecommunication device and having a client account ID stored therein and
- a merchant program application adapted to run on a merchant device and having a merchant account ID stored therein, wherein
  - the payment processing server is configured to receive a processing request from the merchant program application, the processing request including the merchant account ID and transaction-related information including at least a transaction amount,
  - the payment processing server comprises a transaction session engine for starting, in the payment processing server, a transaction session, wherein said transaction session comprises creating and storing, in the payment processing server, a unique transaction code,
the payment processing server is configured to transmit the transaction code to the merchant program application,

- the client program application is configured to interact with input means of the client's mobile telecommunication device to receive the transaction code transmitted from the merchant to the client's mobile telecommunication device,

- the payment processing server is configured to receive from the client program application the transaction code together with the client account ID,

- the payment processing server is configured to transmit the transaction amount to the client program application for displaying the transaction amount,

- the client program application is configured to receive an authorizing input from the client and to transmit an authorization message to the payment processing server,

- the payment processing server is configured to send a clearing request message to the financial institution of the client's and/or the merchant's financial account, to receive a clearing response message and to cause a transfer of the transaction amount from the client's financial account to the merchant's financial account.

12. A computer program product characterized in that it comprises program code which, when loaded into a computer, carries out the method according to any one of claims 1 to 10.

13. Data storing media, comprising program code instructions of a computer entity program according to claim 12.
**INTERNATIONAL SEARCH REPORT**

**International application No**
PCT/IB2013/00Q144

**A. CLASSIFICATION OF SUBJECT MATTER**
INVENTION G06Q20/32 G06Q20/O2 G07F19/00

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

**B. FIELDS SEARCHED**
Minimum documentation searched (classification system followed by classification symbols)
G06Q G07F

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)
EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>EP 1 513 120 A2 (FUN COMM GMBH [DE]) 9 March 2005 (2005-03-09) the whole document</td>
<td>1-13</td>
</tr>
<tr>
<td>X</td>
<td>EP 2 128 809 AI (STALS LUC [DE]; PALZER MARTIN [DE]; HI RASAWA S) 2 December 2009 (2009-12-02) paragraphs [0006], [0009]-[0095]; claims; figures</td>
<td>1-13</td>
</tr>
<tr>
<td>X</td>
<td>US 2010/320266 AI (WHITE SPENCER NEIL [US]) 23 December 2010 (2010-12-23) paragraphs [0009]-[0012]; paragraphs [0030]-[0051]; claims; figures</td>
<td>1-13</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

* 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 application 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
  * **Z** document member of the same patent family

**Date of the actual completion of the international search**
31 July 2013

**Date of mailing of the international search report**
08/08/2013

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

**Authorized officer**
Aguiar, Jose Maria
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>×</td>
<td>EP 2 088 549 A1 (ACCENTURE GLOBAL SERVICES GMBH [CH]), 12 August 2009 (2009-08-12)</td>
<td>1-13</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>EP 1513120 A2</td>
<td>09-03-2005</td>
<td></td>
</tr>
<tr>
<td>EP 2128809 AI</td>
<td>02-12-2009</td>
<td>AU 2009253407 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2765081 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2128809 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2011137797 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2013091059 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wo 2009144010 A1</td>
</tr>
<tr>
<td>US 2010320266 AI</td>
<td>23--12--2010</td>
<td>NONE</td>
</tr>
<tr>
<td>EP 2088549 AI</td>
<td>12--08--2009</td>
<td>NONE</td>
</tr>
<tr>
<td>US 2010211506 AI</td>
<td>19--08--2010</td>
<td>TW 201032160 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010211506 A1</td>
</tr>
</tbody>
</table>