



(51) International Patent Classification:
G06Q 20/32 (2012.01)

(21) International Application Number:
PCT/EP2012/060937

(22) International Filing Date:
8 June 2012 (08.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11169629.0 10 June 2011 (10.06.2011) EP

(71) Applicant (for all designated States except US): **SWED-BANK AB** [SE/SE]; Head of Group Business Support, Brunkebergstorg 8, S-105 34 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **ALFTHAN, Björn** [SE/SE]; Skånegatan 93, S-116 35 Stockholm (SE).

(74) Agents: **JOHANSSON, Anna Olivia** et al.; Venner, Shipley LLP, 200 Aldersgate, London EC1A 4HD (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: ELECTRONIC TRANSACTIONS

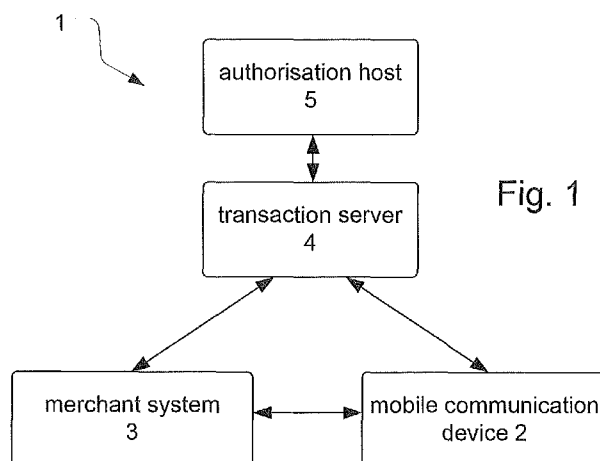


Fig. 1

(57) Abstract: A mobile communication device for facilitating an electronic transaction between a first party, corresponding to a user of the device, and a second party, the device comprising: a memory for storing information corresponding to one or more transaction authorisation tickets, previously received over a communication link from a transaction server, each ticket being associated with unique identification data and providing a one-time authorisation for the user of the mobile communication device to enter into an electronic transaction; a user input interface for receiving at least one transaction parameter associated with a transaction between the first and the second party from the user of the mobile communication device; a code generator for generating a code corresponding to the transaction, the code including the unique identification data of one of said one or more transaction authorisation tickets and the transaction parameter; and an interface for communicating said code to another device to be forwarded to the transaction server, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first party to the second party. There is also provided an apparatus for receiving the code and forwarding the code to a server. Additionally, there is provided a server for processing the payment.

Electronic Transactions

Field of the Invention

The invention relates to electronic transactions using mobile communication
5 devices. Particularly, but not exclusively, the invention relates to a mobile
communication device for generating a code corresponding to an electronic
transaction.

Background of the Invention

10 Mobile communication devices, such as smart phones, are becoming more and
more powerful in terms of the functionality they provide. A number of proposals
have been made for systems that allow mobile communication devices to be used
to make payments or to redeem purchased services and products. It is important
that the systems allow the transactions to be carried out quickly and securely.

15 Many existing methods and systems for carrying out financial transactions using
mobile communication devices require that a payment is made well before the
products and services are redeemed and the mobile communication device is only
used to provide proof of purchase. These methods and systems cannot be used
20 when a user does not know what he wants to buy or the prices of the products and
services he desires before he arrives at the location where the products and
services are sold, for example in a supermarket or a restaurant. Existing, secure
methods that allow payments to be made at the point of sale typically require the
mobile communication device to connect to a network at the point of sale. This is
25 of course a problem if the purchase is made in a location with no network access
or where only a very slow network connection is available.

Some method and systems for carrying out electronic transactions using mobile
communication devices use barcodes displayed on the screens of the mobile
30 communication devices to communicate transactional information to the merchant
terminal. More specifically, WO 01/93120 discloses a system that uses a barcode
displayed on a screen as proof of purchase. A mobile communication device can
receive the barcode in an SMS or access the barcode using a universal resource

locator (URL) received from a server. Similarly, US2007/0012765 discloses a system in which a ticket corresponding to an ordered product or service is received in a mobile phone. When the product or service is redeemed, a barcode based on the ticket is generated on the screen and read by the product or service provider. The ticket can be used a multiple of times. The system relies on that the payment is made in advance of the time at which the goods or services are redeemed.

WO2010/065218 discloses a system for carrying out electronic transactions using a mobile communication device. At the point of sale, a mobile telephone number and a password is transmitted to a payment provider system which generates a barcode corresponding to the user's account and sends it to the mobile communication device. The merchant scans the barcode and transmits the barcode information and the purchase information to the payment provider to complete the payment. The barcode may only be valid for a short time, for security purposes, and the mobile communication device needs access to a network at the point of sale. WO2009/070114 discloses an electronic payment system in which a mobile phone can request an electronic cheque from a payment provider, access the electronic cheque in the form of a barcode displayed on a website and provide the electronic cheque to the merchant by displaying it on the screen and allowing it to be scanned. The electronic cheque is only valid for a limited time and the system requires a communication link to be established to the website at or a short time before the point of sale. The owner of the mobile phone further has limited control over how the cheque is used by the merchant.

EP1480476 discloses a mobile communication device configured to generate a barcode including data associated with the subscriber identity to allow a payment to be carried out based on the subscriber identity.

There is a need for a secure system in which a communication link from the mobile device to the payment provider is not needed at the point of sale.

Summary of the Invention

According to the invention, there is provided a mobile communication device for facilitating an electronic transaction between a first party, corresponding to a user of the device, and a second party, the device comprising: a memory for storing
5 information corresponding to one or more electronic transaction authorisation tickets, previously received over a communication link from a transaction server, each ticket being associated with unique identification data and providing a one-time authorisation for the user of the mobile communication device to enter into an electronic transaction; a user input interface for receiving at least one transaction
10 parameter associated with a transaction between the first and the second party from the user of the mobile communication device; a code generator for generating a code corresponding to the transaction, the code including the unique ticket identification data of one of said one or more transaction authorisation tickets and the transaction parameter; and an interface for communicating said code to another
15 device to be forwarded to the transaction server, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first party to the second party.

The mobile communication device may further comprise a receiver for receiving the
20 one or more transaction authorisation tickets from said transaction server over a network prior to the electronic transaction, the code generator being configured to generate the code based on the unique identification data for the transaction authorisation ticket and the transaction parameter without communicating with the transaction server to allow a payment to be made without the mobile
25 communication device requiring access to a communication network.

Since the code generator can generate a code based on previously received transaction authorisation tickets and transaction parameters received from a user, the payment can be made without the mobile communication device requiring a
30 connection to a network at the point of sale. The transaction authorisation tickets can be received at some time before the point of sale. For example, a ticket may be stored for an extended time, for example a few months or even longer before it is used. Moreover, the memory may store a plurality of unused transaction

authorisation tickets at the same time. The user may therefore enter into multiple transactions before a new connection to a network has to be established to receive new transaction authorisation tickets. The merchant system, which typically has access to a more reliable network link than a mobile communication device, can
5 validate a ticket at the point of purchase by exchanging messages with the server that issued the ticket. Since the ticket is unique and can only be used once, the invention ensures that the transaction is secure.

Since the mobile communication device only stores one or a few tickets at any one
10 time, the risk is limited if the mobile communication device is lost. Each transaction authorisation ticket may be limited to a maximum amount. Additionally, since the system allows a user to enter an amount at the point of purchase, the system makes sure that fraud by the merchant is reduced. The graphical code and messages transmitted to the central server are protected by encryption codes, such as SHA
15 256 hash codes and any modification to the graphical code and the information in the graphical code by the merchant will be detected by the central server.

Consequently, the invention provides a secure method of making a payment without the need for a connection to a mobile network at the point of purchase.

20 The at least one transaction parameter may comprise a payment amount. The at least one transaction parameter may further comprises data indicating a selection of a debit or credit card to be used to make the payment. Alternatively, the at least one transaction parameter may further comprise data indicating a selection of an
25 account to make the payment from.

The code generator may be a graphical code generator and the communication interface may be a display for displaying the graphical code to be read by a graphical code reader associated with the other device. The graphical code may be a barcode.
30 The display may comprise a touch screen which provides the user input interface.

According to the invention, there is also provided an apparatus for facilitating an electronic transaction between a first party and a second party corresponding to the

user of the apparatus, the apparatus comprising: a first communication interface for receiving a code from a device associated with the first party, the code including unique identification data, indicating a transaction authorisation ticket, and a transaction parameter, the transaction authorisation ticket providing a one-time
5 authorisation for the first party to enter into an electronic transaction; a processor for generating a message comprising said code; a second communication interface for transmitting said message to a server and for receiving an acknowledge message from the server that a payment has been processed based on information in the transmitted message, the transaction authorisation ticket in combination with the at
10 least one transaction parameter providing an instruction to the transaction server to process a payment from the first to the second party.

The code may be a graphical code and the first communication interface may comprise a graphical code reader. The graphical code reader may comprise a camera.
15 The processor may further be configured to validate at least one of said transaction parameters and in response to determining that the transaction parameter is valid, generate said message.

The at least one transaction parameter in the code may comprises a payment
20 amount to be paid from the first party to the second party and the apparatus may further comprise an interface for receiving a payment amount to be paid from the first party to the second party. The processor may be configured to compare the amount to be paid in the graphical code with the amount to be paid received via the interface and generate said message if the amount to be received matches the
25 amount indicated in the graphical code.

Yet further, according to the invention, there is also provided a server for facilitating an electronic transaction between a first party and a second party, the server comprising: a memory for storing information about a number of electronic
30 transaction authorisation tickets associated with users of a electronic transaction system, each ticket being associated with unique identification data and providing a one-time authorisation for a user of the system to enter into an electronic transaction, each ticket further being associated with information in memory

indicating whether the ticket has been used to make a payment; a communication interface for receiving a message comprising a code for an electronic transaction between the first party and the second party, the code including unique identification data for a transaction authorisation ticket issued to the first party and
5 a transaction parameter for the electronic transaction; a processor arrangement for determining whether the transaction authorisation ticket received in the code has been used, and in response to a determination that the transaction authorisation ticket has not been used, processing a payment from the first party to the second party.

10

Processing the payment may comprise instructing an authorisation host to complete the payment. The processor may also be configured to update the information in memory to indicate that the ticket has been used. The processor may further be configured to issue a new transaction authorisation ticket and the communication
15 interface may be configured to transmit said ticket to a mobile communication device.

Since the ticket is unique and has been issued for the first party, the server may determine the identity of the first party based on the unique identification data for
20 the ticket.

According to the invention, there is also provided a system comprising the mobile communication device, the apparatus and the server.

25 Furthermore, according to the invention, there is provided a method of using a mobile communication device to carry out an electronic transaction between a first party, corresponding to a user of the mobile communication device, and a second party, the method comprising: storing one or more transaction authorisation tickets, previously received in the mobile communication device over a communication link
30 from a transaction server, each ticket being associated with unique ticket identification data and providing a one-time authorisation for the user of the mobile communication device to enter into an electronic transaction; receiving at least one transaction parameter associated with a transaction between the first and the second

party from the user of the mobile communication device; generating a code corresponding to the transaction in the mobile communication device, the code including the unique identification data of one of said one or more transaction authorisation tickets and the transaction parameter; and communicating said code to
5 another device to be forwarded to the transaction server, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first to the second party.

According to the invention, there is also provided a method of using an apparatus
10 to facilitate an electronic transaction between a first party and a second party corresponding to the user of the apparatus, comprising: receiving a code from a device associated with the first party, the code including at least one transaction parameter and unique identification data for a transaction authorisation ticket providing a one-time authorisation for the first party to enter into an electronic
15 transaction; generating a message comprising said code; transmitting said message to a server; and receiving an acknowledge message from the server that a payment has been completed based on information in the transmitted message, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the
20 first to the second party.

Moreover, according to the invention, there is also provided a method of operating a server to process an electronic transaction between a first party and a second party, the method comprising: storing information about a number of transaction
25 authorisation tickets associated with users of a electronic transaction system, each ticket being associated with unique identification data and providing a one-time authorisation for a user of the system to enter into an electronic transaction, each ticket further being associated with information in memory indicating whether the ticket has been used to make a payment; receiving a message comprising a code for
30 an electronic transaction between the first party and the second party, the code including a transaction parameter and unique identification data of a transaction authorisation ticket issued to the first party; determining whether the transaction authorisation ticket received in the code has been used; and in response to a

determination that the ticket has not been used, processing a payment from the first party to the second party.

Yet further, according to the invention there is provided a computer program
5 comprising instructions that when executed by a processor causes the process to carry out the methods set out above.

Brief Description of the Drawings

Embodiments of the invention will now be described, by way of example, with
10 reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of an electronic payment system;

Figure 2 is a schematic diagram showing the components of a mobile communication device of the electronic payment system;

Figure 3 is a schematic diagram showing the components of a merchant system of
15 the electronic payment system;

Figure 4 is a schematic diagram showing the components of a transaction server of the electronic payment system;

Figure 5 illustrates a process in the mobile communication device for making a payment;

20 Figure 6 illustrates a process in the merchant system for receiving a payment;

Figure 7 illustrates the data flow to and from the mobile communication device;

Figure 8 illustrates a process in the transaction server for processing a payment;

Figure 9 illustrates interactions in a payment system comprising two transaction servers;

25 Figures 10 and 11 illustrate a process of signing up to a service that allows a user of a mobile communication device to make payments using the mobile communication device;

Figure 12 illustrates a process of receiving a payment using a mobile communication device; and

30 Figure 13 shows the components of an extended system for carrying out electronic transactions.

Detailed Description

With reference to Figure 1, a system 1 for carrying out electronic financial transactions comprises a mobile communication device 2, a payment reception system 3, a transaction server 4 and a payment authorisation host system 5. The mobile communication device 2 may be a mobile telephone or a personal digital assistant (PDA). The payment reception system may, for example, be a merchant system such as a cash register and a card reader system. The authorisation host system 5 may be a card authorisation system, such as VISA or MasterCard, or a bank. It should be noted that although a single transaction server is shown, the transaction server 4 may comprise more than one server. It may comprise a network of servers operated by the same operator or a number of servers and/or network of servers operated by different operators. A user of the mobile communication device 2 can use the mobile communication device to make an electronic payment to a merchant operating the merchant system.

At some time, before the user intends to make a payment, a communication link is established between the transaction server 4 and the mobile communication device 2 and one or more electronic transaction authorisation tickets are received and stored in the mobile communication device 1. A transaction authorisation ticket is a one-time authorisation for a user of the mobile communication device to enter into an electronic transaction. More specifically, a transaction authorisation ticket is an authorisation for a single electronic payment to another party. The tickets may be received by any suitable method, including but not limited to a Short Message Service (SMS) or Internet Protocol (IP). The communication link includes a mobile communication network operated by a mobile communication network operator.

At a later time, at the point of sale, the user operates the mobile communication device 2 to generate a code for the financial transaction. The code is based on a ticket previously received and a number of transaction parameters. The code is communicated to the merchant system 3. The merchant system 3 then contacts the transaction server 4 to validate the code and process the payment. After having validated the code, the transaction server 4 provides the necessary information to

the authorisation host 5 to complete the payment. The merchant system 3 may communicate with the transaction server 4 via a wired or wireless communication network or a combination of a wired and a wireless communication network. Similarly, the transaction server 4 may communicate with the authorisation host 5
5 via a wired or wireless communication network or a combination of a wired or wireless network. Acknowledgements of the transactions are then sent to the merchant system 3 and the mobile communication device 2.

Since the code can be generated in the mobile communication device based on a
10 ticket previously received and without the mobile communication device accessing a communication network to communicate with the server 4, the mobile communication device can be used to make a payment even if there is no access to a communication network. The merchant system needs to be connected to a network to validate the code but the merchant system is likely to have a more
15 reliable connection to a network anyway.

With reference to Figure 2, the mobile communication device 2 may be in the form of a smart phone. The mobile communication device comprises a speaker 6, a microphone 7, a display 8, and a key pad 9. The display 8 may be a touch screen
20 and in some embodiments the key pad 9 may be provided by the touch screen. The mobile communication device can communicate through one or more mobile networks, which may include but are not limited to GPRS, GSM, and CTMA. The mobile communication device can therefore receive data both in SMS messages and over IP. To this end, the mobile communication device 2 also comprises a
25 radio frequency (RF) communication interface 10 and a codec 11. The RF communication interface 10 may comprise one or more antennas and an RF stage for receiving and processing signals. The codec 11 translates signals received via the RF communication interface 10 into a format that can be communicated to a user of the mobile communication device via the speaker 6 and display 8.
30 Similarly, audio and data signals generated in the mobile communication device 2 can be processed by the codec 11 into a form that can be transmitted by the RF communication interface 10.

The components of the mobile communication device are controlled by a microcontroller 12. The mobile communication device also comprises a memory 13 for storing data and instructions. The memory may include a Subscriber Identify Module (SIM) card and, for example, a flash memory. In some

5 embodiments, the controller may run an Android, iOS, Windows Mobile, Blackberry or Symbian operating system. However, it should be realised that the above operating system are just examples and any suitable operating system for the mobile communication device can be used.

10 According to embodiments of the invention, the mobile communication device will also comprise a graphical code generator 14 as will be described in more detail below. Additionally, the mobile communication device may comprise a camera 15, as will also be described in more detail below.

15 The memory 13 may store a number of software applications. According to the invention, one of the software applications 16, when run by the controller 12, allows a user to make a payment with the mobile communication device. The application may include a graphical user interface for allowing a user to make the payment. The application may also comprise instructions for communicating with

20 the display 8, the camera 15, the graphic code generator 14, the codec 11 and the RF communication interface 10. In some embodiments, the graphical code generator 14 may form a part of the application 16 instead of being a separate entity. The application may also be responsive to instructions from the keypad 9. Additionally, the application may also comprise an algorithm for generating a code

25 for authenticating messages transmitted using the application. The algorithm may generate an encryption code. The algorithm may for example be a Secure Hash Algorithm (SHA) 256 algorithm that uses a salt based on at least a shared secret key. The application is associated with a memory area 17 for storing a password for the application, one or more electronic tickets each authorising the mobile

30 communication to make a payment, transaction parameters for carrying out payments and any other data required to use the application and make secure electronic payments.

With respect to Figure 3, the merchant system 3 comprises a network communication interface 18 for communicating with remote systems, such as a transaction server and an authorisation host. The network communication interface 29 may comprise an interface for sending and receiving data to and from the remote systems via the Internet. For example, the network communication interface may send and receive messages using Hypertext Transfer Protocol Secure (HTTPS). However, it should be realised that the network communication interface may send and receive messages using any suitable protocol and network. The merchant system 3 also comprises a merchant communication interface 19.

10 The merchant communication interface 19 may comprise a display, and a keypad or any other suitable means for communicating with an operator of the system. The display may provide a touch screen and the keypad may be provided by the touch screen. The merchant system also comprises a controller 20 for controlling the network communication interface and the merchant communication interface.

15 Additionally, the merchant system comprises a memory 21 for storing instructions and data. The merchant system may be a PC or a dedicated payment terminal in, for example, a shop. When the merchant system is a dedicated payment terminal it may also comprise a card payment terminal 22 under control of the controller for taking card payments. Additionally, according to embodiments of the invention,

20 the merchant system comprises a graphic code reader 23 as will be described in more detail below.

The merchant system stores a computer program 24 in memory 21 comprising instructions that when executed by the controller processes payments received in the system from mobile communication devices. The computer program may include instructions for generating a code for authenticating messages transmitted using the merchant system and for validating authentication codes of messages received in the merchant system. The memory 21 may also store transaction details for past payments.

30

The main tasks of the transaction server 4 are to process payments and to control the user accounts of the users of the system. With reference to Figure 4, the transaction server 4 comprises one domain 25 for the processing tasks required

for the seller account in a transaction and one domain 26 for the processing tasks required for the buyer account of a transaction. In some embodiments, the seller domain 25 and the buyer domain 26 can be separate servers and may even be located remotely, as will be described in more detail below with respect to Figure 5 9. Each domain 25, 26 has its own controller and associated memory. The memories stores instructions that when executed by the controllers allow payments to be processed. The two domains may exchange secure messages.

The transaction server 4 also comprises a database 27, a security module 28 and a 10 network communication interface 29. The database stores details of the user accounts held by users of the system. It may for example store the names, contact information and account and/or card details for the users. It will also store information about transaction authorisation tickets sent to buyers, as will be described in more detail below. In some embodiments, the database engine for the 15 database 27 may comprise, but is not limited to, a MySQL engine. The security module is accessed to encrypt and decrypt messages exchanged between the domains 25, 26, with other transaction servers and with the payment authorisation host 5. The security module may also be configured to ensure that messages are securely exchanged with the merchant system 3. Additionally, the security module 20 may also be configured to ensure that messages are securely exchanged with the mobile communication device 2. The network communication interface 29 may comprise an interface for sending and receiving data via the Internet. For example, the network communication interface 29 may send and receive messages using Hypertext Transfer Protocol Secure (HTTPS). However, it should be realised that 25 the network communication interface 29 may send and receive messages using any suitable protocol and network.

A process for carrying out a payment using the mobile communication device will now be described with respect to Figures 5, 6, 7 and 8. With reference to Figures 30 5 and 7, at some stage the mobile communication device receives one or more payment authorisation tickets 30 from the transaction server (step 5.1) and stores them in the application memory area 17. A ticket is an authorisation to enter into a financial transaction, to be used only once by the receiving mobile

communication device 2. Once a ticket has been invoked by a user, the ticket is exhausted. The ticket may be associated with unique identification (ID) data provided as a unique string of numbers, letters or a combination of numbers and letters. In other words, each ticket received in the mobile communication device is
5 associated with different identification data. The information received from the server comprises the unique identification data. In some embodiments, the ticket only consists of the unique string or other unique identification data. The unique identification data, which will also be referred to as the ticket ID, is also stored in the database 27 of the transaction server. The database 27 also stores an indication
10 of whether a transaction authorisation ticket has been used. For example, the record for each ticket may include a field that can have two values, a first value indicating that the ticket has been invoked by a user and a second value indicating that the ticket has not yet been invoked by a user. The ticket can be considered analogous to a blank cheque in that it allows a user to make a payment for an
15 amount to be decided by the user and that it can be used only once. The ticket may be received via the RF communication interface 10 of the mobile communication device 2 as, for example, an SMS message or as an IP message. Depending on the settings, a mobile communication device may be allowed to store a single unused ticket or a plurality of unused tickets at the same time. The number of tickets 30 a
20 mobile communication device can store simultaneously may be set by the service provider or by the user of the mobile communication device and may be different for different users and mobile communication devices. The ticket is protected by a password also stored in the application memory area 17 of the mobile communication device.

25
Some time later, the user initiates the payment application (step 5.2). The initiation may involve opening the application and entering log-in information. The log-in information may comprise a password. Once the password has been validated against the password stored in the memory 17, the mobile
30 communication device 2 is ready to receive instructions to make a payment. The user may select an option on the graphical user interface of the application to indicate that a payment is required and choose one or more parameters (step 5.3). For example, the user may indicate from which of one or more accounts or one or

more credit or debit card payments the user wants to make the payment. The user may also indicate in which currency he would like to make the payment. In some embodiments, the currency may be a fixed parameter that may not be changed by the user. In other embodiments, the currency may be chosen by the user when he
5 makes a payment. It is contemplated that in some embodiments, a recommendation or a decision about a currency may be made based on the location of the mobile communication device. The location may be automatically determined using a location service such as a global positioning system (GPS).

10 The application then prompts the user for the amount the user wants to pay. The user may for example be at the check-out of a supermarket and the cashier may have told the user the total price of the products the user desires to purchase. The mobile communication device receives an indication of the amount from the user (step 5.4) and instructions to proceed with the payment.

15 The application then generates a graphical code 31 for the payment based on the amount, the ticket that is being used for the payment and any other parameters required (step 5.5). The application may instruct the graphical code generator 14 to generate the code and to display the generated graphical code (step 5.6). In
20 some embodiments, the graphical code is a barcode. The barcode may be a QR code. However, it should be realised that any suitable barcode may be used. The graphical code includes at least the identification data for the ticket and the amount to be paid. The graphical code may also include an indication of the time the graphical code was generated, the currency used for the payment, the version
25 of the application used and identification details of the server that issued the ticket. The graphical code may also include a SHA256 code and a checksum. It should be realised that the graphical code can include any information required for the purchase. By including additional information in the code such as the time of generation and the cell id of the mobile phone when the code was generated,
30 security may be improved.

The user then presents the mobile communication device 2 to the merchant system 3 for the graphical code to be read (step 5.6). If the code is validated, the

mobile communication device receives a receipt for the transaction (step 5.7). The receipt may be accompanied with a new payment authorisation ticket (step 5.1) to allow the user to make a new payment. Alternatively, the new ticket may be sent separately.

5

Once a ticket has been used, it is contemplated that a user of the mobile communication device cannot select the ticket again. For example, it may be deleted from the memory or the memory may include an indication that it has been used.

10

It should be realised that the mobile communication device only needs to communicate over a network at step 5.1 and step 5.7. The other steps can be carried out without any access to any communication network. Consequently, the mobile communication device does not need to have access to a communication network at the point of sale. The dashed lines in Figure 5 indicate that an

15

extended time can pass between the steps connected by the dashed lines.

Consequently, the tickets can be received at some point before the purchase and the receipts can be received at some point after the purchase when the mobile communication device has access to a communication network. When the mobile

20

communication device does not have access to a network, the number of payments a mobile communication device can make is only limited by the number of tickets stored in the mobile communication device. It should be realised that if more than one payment is carried out in a row, steps 5.3 to 5.6 can be repeated until all the payments have been made, provided that the mobile communication device

25

stores a sufficient number of tickets.

The merchant system operator will at some point before the transaction initiate the merchant system 3. The merchant system operator may inform the buyer of a price, which the operator may also enter into the merchant system 3 using the merchant communication interface 19. With reference to Figure 6 and 7, when the graphical code 31 is presented to the operator, the operator uses the graphical code reader 23 to read the code (step 6.1). When the graphical code reader comprises a camera, the operator uses the camera to scan the graphical code. The

30

camera may take a photo of the graphical code. The controller 20 of the merchant system then interprets the graphical code and extracts information required to process the payment (6.2). The program for processing payments may include a graphical code interpreter to interpret the graphical code. In the embodiments

5 when the graphical code is a barcode, the program comprises instructions for interpreting the barcode. The controller 20 extracts the payment amount indicated in the code and the operator of the merchant system is prompted to validate the payment amount. If the payment amount equals the price, the operator of the merchant system may confirm that the payment amount is correct using the

10 merchant communication interface 19 (step 6.3). In some embodiments, it is considered that the merchant system can validate the payment amount automatically by comparing the price to a total price calculated in the cash register for a number of products and/or services.

15 When the amount is confirmed, the controller then generates a message (step 6.4), including the graphical code, and sends the message to the transaction server. In addition to the graphical code, the message may also include identification details for the merchant. Since the code is sent in its entirety, it is more difficult for a merchant to commit fraud. By analysing the SHA256 code and the checksum in

20 the transaction server, the transaction server can check that the message has not been tampered with. The message may also be protected by an encryption code or other information used to authenticate the message, for example another SHA256 code.

25 At some point later, the merchant system receives an acknowledgement (step 6.5) from the transaction server 4. If the graphical code has been validated and the transaction has been completed, the acknowledgement will be a receipt for the transaction. However, the payment was not accepted, the acknowledgement may be replaced by a message informing the merchant that the transaction could not be

30 completed. Typically, it would take less than 4 seconds between the time the message is sent to the transaction server and the time the acknowledgement is received. In the embodiments wherein the merchant system comprises a card payment terminal, the information in the acknowledgement message may be

included in the card transaction information and processed in the same way as if the payment would have been made using a credit or debit card. The same electronic transaction program may be configured to handle both the card payment and graphical code payments. For example, when an operator selects an option on a graphical user interface to receive a payment, the electronic transaction program opens both the card terminal and the web-camera (if not already open). The first unit to register payment data transfers the data to the electronic transaction program. Alternatively, the operator can choose, using the graphical user interface, whether to take the payment using the card terminal or the graphical code reader or to receive the payment in cash. In other embodiments, a separate electronic transaction program may be configured to handle the graphical code payments and may communicate information about the completed transaction to the card payment program once the graphical code transaction has been completed. In some embodiments, the graphical code payments may be handled completely separately from the card payments in the merchant system.

With reference to Figure 8, the transaction server 4 receives a payment message from a merchant system (step 8.1). In some embodiments, the same transaction server is used by the buyer and the seller. However, in other embodiments the buyer and the server are registered with different transaction servers as will be described in more detail below. The message is forwarded from the network communication interface 29 to the seller domain 26. The seller domain carries out a validation of the seller (step 8.2). The validation may include a determination that the seller is registered with the server. The seller domain can carry out this check by accessing the records in the database 27. The validation may also include an analysis of the authentication information in the message, such as a SHA256 hash code of the message. A message is then sent from the seller domain to the buyer domain. Identification details for the transaction server 4 for the buyer may for example have been included in the code and may be extracted by the seller domain. A message, comprising the graphical code, may then be transmitted to the transaction server identified in the graphical code. The seller domain may include another authentication code, such as a SHA256 hash code in the message.

When the buyer and seller are registered with the same server, the message is an internal message. The buyer domain receives the message and checks the authenticity of the graphical code (step 8.4). For example, the buyer domain may
5 check that the graphical code has not been modified by checking the SHA256 hash value and the checksum of the graphical code. If it is determined that the graphical code is not authentic, the buyer domain reports back that the payment cannot be processed (step 8.3). It may send a message to the seller domain for the seller domain to report back to the merchant system. If the graphical code is
10 validated, the buyer domain extracts the ticket ID from the code and validates the ticket (step 8.4). The buyer domain may check whether a ticket with the ticket ID indicated in the transaction message exists in the database 27. The buyer domain also checks whether the ticket has not been exhausted. If the ticket has been exhausted, the buyer domain reports back to the seller domain and in turn the
15 merchant system that the ticket is invalid (step 8.3). If the ticket has not been exhausted the buyer domain updates the record for the ticket to indicate that the ticket has now been used (step 8.6). Since the ticket is “exhausted” as soon as it has been invoked once by the mobile communication device, the security of the system is improved. The buyer domain also validates the buyer (step 8.7). The
20 validation may involve checking whether the buyer is still registered. The identity of the buyer may be determined based on the ticket ID. The buyer domain can carry out these checks by accessing the records in the database 27. The validation in the buyer domain 26 may also involve checking the SHA256 hash code of the message received from the seller domain.

25

When the message has been validated, the buyer domain retrieves payment information for the seller required to complete the transaction and sends the information to the seller domain (step 8.8). For example, card or account information may be obtained from the database 27 and sent to the seller domain
30 25. The payment information may be retrieved in dependence on the parameters indicated in the code. If the code indicates that a specific debit or credit card is to be used, the buyer domain may retrieve and encrypt the card details using the security module 28. The seller domain decrypts and encrypts the card number

using the security module 28, includes it in a card authorisation transaction message and sends it to the authorisation host (step 8.9). In the case when the payment is generated using a debit or credit card, the authorisation host may be a card payment system. If the payment is made from a user's account, the
5 authorisation host may be a bank. A SHA256 hash code, or any other suitable authentication code, may also be included in the message.

A message from the authorisation host 5 is then received via the communication interface 29 some time later and indicates whether the payment can be completed
10 (step 8.10). For example, if the seller does not have sufficient money in his account or a card has been cancelled but this has not been updated in the transaction server, the payment may be stopped by the authorisation host. If the payment is accepted, the message from the authorisation host is an acknowledgment that the transaction has been processed. The message may
15 comprise the necessary receipt and debit data. On receipt of the message, the seller domain sends an acknowledgement and receipt data to the merchant system (step 8.11). The message may be protected by an authentication code, such as a SHA256 hash code. The seller domain 25 also sends a message that confirms that the transaction has been completed to the buyer domain 26. The buyer domain, on
20 receipt of the message, forwards a receipt to the mobile communication device 2 (step 8.12). The seller domain 25, on receipt of the message, may also issue a new ticket to the buyer. The seller domain 25 may forward the ticket to the mobile communication device with the receipt (step 8.13). The new ticket and the receipt are delivered to the mobile communication device 2 by the mobile communication
25 network operator.

Figure 8 has been described above with respect to a transaction for which both the buyer and the seller are registered with the same server. However, the buyer and seller may also be registered in different servers. In that case, the seller
30 domain of the seller's transactional server 4a and the buyer domain of the buyer's transactional server 4b exchange messages, as shown in Figure 9, via the network communication interfaces of the transaction servers 4a, 4b. The buyer communicates the graphical code to the seller (action a). The seller then sends a

message to its transaction server (action b) and the seller domain of the transaction server validates the message and the buyer (action c) with respect to the database of the seller transaction server. The seller transaction server then sends a message to the buyer transaction server (action d). The buyer transaction
5 server validates the message, the graphical code, the ticket and the buyer with respect to the database of the buyer transaction server and updates the status of the invoked ticket (action e). The buyer transaction server sends a message back to the seller transaction server (action f), which instructs the authorisation host to process the payment (action g). The authorisation acknowledges the instructions
10 to the seller transaction server (action h) and the seller domain of the seller transaction server communicates that the payment has been accepted to the buyer transaction server (action i) and the seller (action j). The buyer domain of the buyer transaction server then sends a receipt (action k) and a new ticket (action l) to the buyer. Of course, the buyer domain may also update the database with the
15 details of the new ticket.

For clarity, Figure 9 does not show the network communication interfaces 29 or the security module 28 but it should be realised that all messages between the transaction servers, the authorisation host and the buyer and seller may be
20 transmitted or received through a network communication interface and include a authentication code generated by the relevant security module, such as a SHA256 hash code created using a salt based on a shared secret key.

It should be realised that different transaction servers may be linked to different
25 authorisation hosts. The different authorisation hosts may also communicate to ensure that the payments are carried out. In some embodiments, a transaction server may be integrated in an authorisation host system. It is contemplated some authorisation hosts may want to operate their own transaction server whereas other authorisation hosts rely on transaction servers operated by other parties. It
30 is also contemplated that companies other than banks and card payment systems may want their own transaction servers.

A transaction was described with respect to Figure 8 to be registered on a card and the authorisation host is then a card authorisation system. However, it should be realised that transactions may also be registered directly on accounts held by the seller and buyer at the authorisation host. In that case, the authorisation host may, 5 for example, be a bank, a large department store or supermarket.

A method of signing up for the payment service will now be described with respect to Figures 10 and 11. The user may use a computer linked to the service provider's system to register for the service. The steps carried out by the service 10 provider's system are shown in Figure 10 and the steps carried out using the mobile communication device 2 are shown in Figure 11. The service provider's system may be provided by a transaction server 4 or may be separate from a transaction server. The user needs to register for the service and accesses the web site of the service provider on the computer and submits a request to register for 15 the service. When the service provider is a bank, it is contemplated that the user may submit the request through the graphical user interface offered by the bank's online banking service. For example, the user may log in to his online banking service and choose an option to register for a mobile communication device payment service. As part of the request, the user may submit details of the mobile 20 communication device. For example, the user may submit his mobile telephone number. He may also submit the International Mobile Subscriber Identity (IMSI number) associated with the SIM card of the mobile communication device and an identification number for the mobile communication device, such as an IMEI number or a UDID number depending on the operating system of the mobile 25 communication device. If the service provider does not already have access to the contact details and bank details of the user, the user would also have to submit these details.

The service provider receives the request (step 10.1) and the identification details 30 entered by the user. In some embodiments, the service provider will need to check that the user has access to the mobile communication device and sends a message with a pin code to the mobile communication device (step 10.2). The message may be transmitted as an SMS. When the user receives the message, the user enters the

pin code in the graphical user interface of the service provider's website and the service provider validates the pin code received (step 10.3). The web site may also ask the user to choose a password for the service. Based on the information received, the service provider then generates a graphical code, such as a barcode
5 and displays it on the screen.

The user has downloaded the application for carrying out a transaction on his mobile communication device (step 11.1). The user opens the application (step 11.2) and uses the camera to scan the graphical code displayed on the computer
10 and extract the parameters in by the code (step 11.3). The application then configures the application based on the extracted parameters (step 11.4). The parameters in the code include all parameters needed for the mobile communication device to configure the application. The parameters may for example include a password chosen by the user, the telephone number associated
15 with the mobile communication device and the default currency to be used by the mobile communication device when making payments. The parameters may also include a shared secret key for generating authorisation codes. Once the application has been configured, the application is ready to be used as described with respect to Figure 5. It is contemplated that the transaction server sends one
20 or more tickets to the mobile communication device immediately or shortly after the user has registered for the service and the application has been configured.

It should be realised that the processes described with respect to Figures 10 and 11 are just examples and variations are contemplated. For example, the service
25 provider may not send an SMS to the mobile communication device with a pin code that the user of the mobile communication device then has to enter to register. In some embodiments, the user would not even have to use a computer to register. The user may instead register by, for example, accessing the service provider's website using the mobile communication device.

30

It has been described above how a merchant system 3 can be used to take a payment from a mobile communication device. However, in some embodiments, a payment can also be received using a mobile communication device. In some

embodiments, when a user registers for the service, the user is registered to both make and receive payments. It is contemplated that the user can indicate whether she wants one or both of these services. With reference to Figure 12, to receive a payment the user opens the payment application 16 (step 12.1) and selects an
5 option indicating that she wants to make a payment. The mobile communication device 2 receives instructions to initiate a payment (step 12.2) and prompts the user to enter the amount to be received. When the user has entered the amount, the mobile communication device notes the amount (step 12.3) and opens the camera application. When the user has scanned the graphical code offered by the
10 other mobile communication device using the camera 15 (step 12.4), the payment application 16 extracts and interprets the information in the barcode (step 12.5) and validates the data. As part of the validation, the mobile communication device may compare the amount indicated in the barcode with the payment amount entered by the user earlier (step 12.6). The payment application then generates and
15 transmits a message to the transaction server (step 12.7). The message includes the scanned code and may also include identification details for the mobile communication device and/or the user of the mobile communication device. In some embodiments, it is contemplated that the identification details for the user and the mobile communication device can be determined based on the mobile
20 phone number at the transaction server 4.

The payment is handled in the same way as if the payment was received by a merchant system, as described with respect to Figure 8. However, the acknowledgement that the payment has been received is sent to the mobile
25 communication device receiving the payment and not to a merchant system. Moreover, the acknowledgement may include different information to the acknowledgement sent to the merchant system since the receipts will be processed in different ways as would be understood by the person skilled in the art. The mobile communication device receives the acknowledgement (step 12.8) and
30 indicates to the user that the payment has been received. It may then update a memory with the transaction information. Alternatively, it receives a message from the transaction server indicating that the payment could not be processed.

Steps 12.4 to 12.8 of the method of receiving a payment using a mobile communication device, described with respect to Figure 12, correspond to steps 6.1 to 6.5 of the method of receiving a payment in the merchant's system.

However, in the embodiment described with respect to Figure 12, the payment

5 amount extracted from the graphical code is compared to a payment amount previously received from a user instead of comparing it to a calculated total or asking the user to confirm that the payment amount is correct. It should be realised that variations are contemplated to the two methods and the payment amounts can be validated in different ways. The user can enter the amount before
10 or after the graphical codes are scanned and the payment amounts can be automatically validated or validated manually by the user.

With reference to Figure 13, an extended system for carrying out electronic

transactions is shown. The system comprises a number of transaction servers 4a,

15 4b, 4c operated by authorisation hosts or other parties. The system also comprises a number merchant systems 3a, 3b belonging to different servers. However, it should of course be realised that a large number of merchant systems can be registered with the same server. The system also comprises a number of mobile communication devices 2a, 2b, the users of which have access to computers 32a,
20 32b for signing up for the service. The mobile communication devices can make payments to each other or to the merchant systems. It is also contemplated that a user can make a payment on a personal computer 33 directly. The personal computer may scan a graphical code, including identification data for a ticket and transaction parameters, from a mobile communication device or generate the
25 graphical code to be sent to a merchant system over the Internet. Moreover, a personal computer 34 may function as a merchant system and receive the graphical code over the Internet.

It has been described that the graphical user interface for the payment applications

30 can be used to initiate a payment. In some embodiments, the graphical user interfaces can also be used to access information about past transactions.

Whilst specific examples of the invention have been described, the scope of the invention is defined by the appended claims and not limited to the examples. The invention could therefore be implemented in other ways, as would be appreciated by those skilled in the art.

5

It should be realised that although it has been described that the code is communicated to the merchant's system by displaying the code to be read by a code reader, the code could also be communicated using a short-range communication network such as a near field communication network.

10

Also, it should be realised that although the graphical code and the messages exchanged in the systems have been described to be protected by SHA256 hash codes, any suitable encryption code or authentication code can be used.

15 Additionally, although it has been described that the records in the database of the transaction server are updated to indicate that a ticket is exhausted as soon as the ticket has been invoked, it is contemplated that the record can be updated to indicate that a ticket is exhausted after the payment has been processed and an acknowledgement has been received from the seller domain. It is further possible
20 that the status of a ticket can have one of a number of values. For example, the record may indicate that a ticket has been sent but not been used, is being processed or has been exhausted.

Furthermore, although the mobile communication device has been described with
25 respect to a smart phone it can be any suitable mobile communication device that can communicate with a transaction server over a mobile communication network or, for example, a wireless network and the Internet. For example, the mobile communication device may be a laptop or a tablet computer.

Claims

1. A mobile communication device for facilitating an electronic transaction between a first party, corresponding to a user of the device, and a second party, the
5 device comprising:
- a memory for storing information corresponding to one or more electronic transaction authorisation tickets, previously received over a communication link from a transaction server, the or each ticket being associated with unique ticket identification data and providing a one-time authorisation for the user of the mobile
10 communication device to enter into an electronic transaction;
 - a user input interface for receiving at least one transaction parameter associated with a transaction between the first and the second party from the user of the mobile communication device;
 - a code generator for generating a code corresponding to the transaction, the
15 code including the unique identification data of one of said one or more transaction authorisation tickets and the transaction parameter; and
 - an interface for communicating said code to another device to be forwarded to the transaction server, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to
20 process a payment from the first party to the second party.
2. A mobile communication device according to claim 1, further comprising a receiver for receiving the one or more transaction authorisation tickets from said transaction server over a network prior to the electronic transaction, the code
25 generator being configured to generate the code based on the transaction parameter and the unique identification data for the transaction authorisation ticket without communicating with the transaction server to allow a payment to be made without the mobile communication device requiring access to a communication network.
- 30 3. A mobile communication device according to claim 1 or 2, wherein the at least one transaction parameter comprises a payment amount.

4. A mobile communication device according to claim 3, wherein the at least one transaction parameter further comprises data indicating a selection of a debit or credit card to be used to make the payment.

5 5. A mobile communication device according to any one of the preceding claims, wherein the code generator is a graphical code generator and the communication interface is a display for displaying the graphical code to be read by a graphical code reader associated with the other device.

10 6. An apparatus for facilitating an electronic transaction between a first party and a second party corresponding to the user of the apparatus, the apparatus comprising:

a first communication interface for receiving a code from a device associated with the first party, the code including unique identification data corresponding to a transaction authorisation ticket and at least one transaction parameter, the
15 transaction authorisation ticket providing a one-time authorisation for the first party to enter into an electronic transaction;

a processor for generating a message comprising said code;

a second communication interface for transmitting said message to a server
20 and for receiving an acknowledge message from the server that a payment has been processed based on the information in the transmitted message, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first to the second party.

25

7. An apparatus according to claim 6, wherein the processor is further configured to validate at least one of said at least one transaction parameters and in response to determining that the transaction parameter is valid, generate said message comprising said code, the code comprising a graphical code and the first
30 communication interface comprising a camera.

8. An apparatus according to claim 6 or 7, wherein the at least one transaction parameter in the code comprises an amount to be paid from the first party to the second party and the apparatus further comprises an interface for receiving a payment amount to be paid from the first party to the second party, wherein the processor is configured to compare the amount to be paid in the graphical code with the amount to be paid received via the interface and generate said message if the amount to be received matches the amount indicated in the graphical code.

9. A server for facilitating an electronic transaction between a first party and a second party, the server comprising:

a memory for storing information about a number of electronic transaction authorisation tickets associated with users of a electronic transaction system, each ticket being associated with unique ticket identification data and providing a one-time authorisation for a user of the system to enter into an electronic transaction, each ticket further being associated with information in memory indicating whether the ticket has been used to make a payment;

a communication interface for receiving a message comprising a code for an electronic transaction between the first party and the second party, the code including the unique ticket identification data of a transaction authorisation ticket issued to the first party and a transaction parameter for the transaction;

a processor arrangement for determining whether the transaction authorisation ticket received in the code has been used, and in response to a determination that the transaction authorisation ticket has not been used, processing a payment from the first party to the second party.

10. A server according to claim 9, wherein the processor is further configured to update the information in the memory to indicate that the transaction authorisation ticket has been used and issue a new transaction authorisation ticket, the communication interface being configured to transmit said ticket to a mobile communication device.

11. A system comprising a mobile communication device according to any one of claims 1 to 5, an apparatus according to claim 6, 7 or 8 and a server arrangement according to claim 9 or 10.

5 12. A method of using a mobile communication device to carry out an electronic transaction between a first party, corresponding to a user of the mobile communication device, and a second party, the method comprising:

storing one or more transaction authorisation tickets, previously received in the mobile communication device over a communication link from a transaction
10 server, each ticket being associated with unique identification data and providing a one-time authorisation for the user of the mobile communication device to enter into an electronic transaction;

receiving at least one transaction parameter associated with a transaction between the first and the second party from the user of the mobile communication
15 device;

generating a code corresponding to the transaction in the mobile communication device, the code including the unique identification data of one of said one or more transaction authorisation tickets and the transaction parameter; and
20 communicating said code to another device to be forwarded to the transaction server, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first to the second party.

25 13. A method of using an apparatus to facilitate an electronic transaction between a first party and a second party corresponding to the user of the apparatus, comprising:

receiving a code from a device associated with the first party, the code indicating at least one transaction parameter and unique identification data
30 corresponding to a transaction authorisation ticket providing a one-time authorisation for the first party to enter into an electronic transaction;
generating a message comprising said code;
transmitting said message to a server; and

receiving an acknowledge message from the server that a payment has been completed based on information in the transmitted message, the authorisation ticket in combination with the at least one transaction parameter providing an instruction to the transaction server to process a payment from the first to the second party.

5

14. A method of operating a server to process an electronic transaction between a first party and a second party, the method comprising:

storing information about a number of transaction authorisation tickets associated with users of a electronic transaction system, each ticket being associated with unique identification data and providing a one-time authorisation for a user of the system to enter into an electronic transaction, each ticket further being associated with information in memory indicating whether the ticket has been used to make a payment;

receiving a message comprising a code for an electronic transaction between the first party and the second party, the code indicating a transaction parameter and the unique identification data of a transaction authorisation ticket issued to the first party;

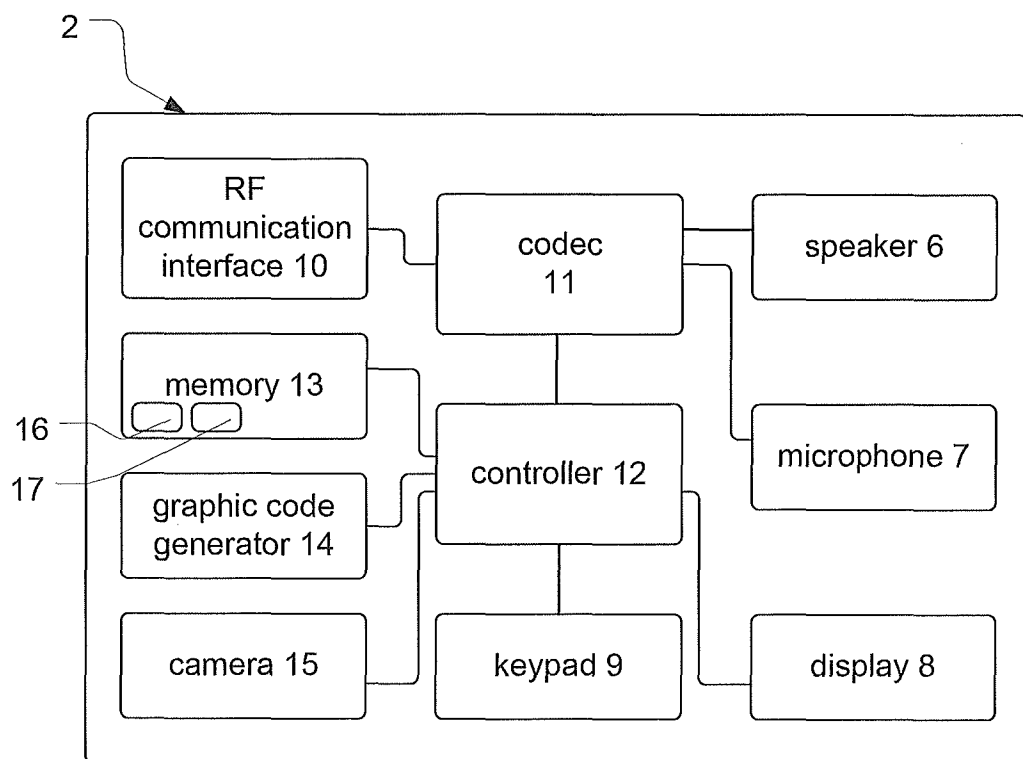
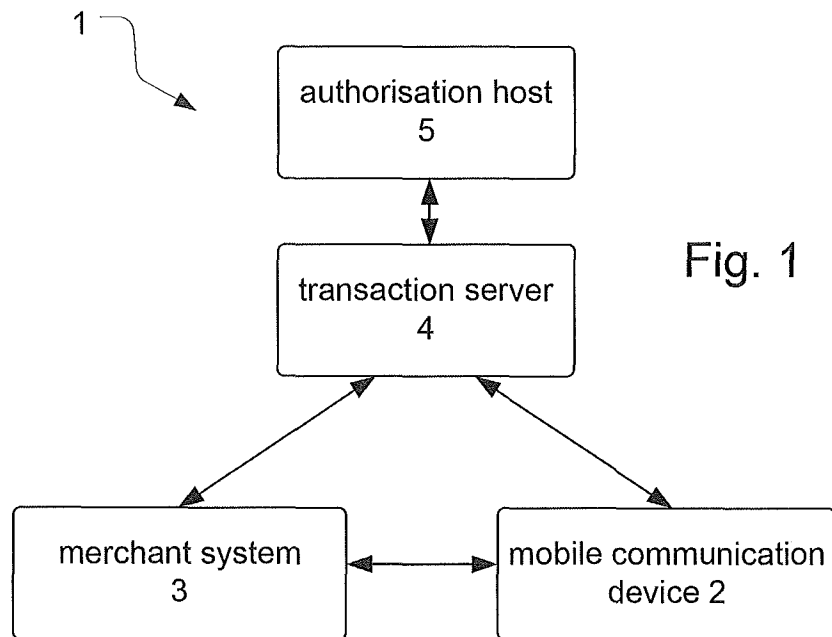
determining whether the transaction authorisation ticket received in the code has been used; and

in response to a determination that the ticket has not been used, processing a payment from the first party to the second party.

15. A computer program comprising instructions that when executed by a processor causes the processor to carry out the method of any one of claims 12, 13 or 14.

25

1/7



2/7

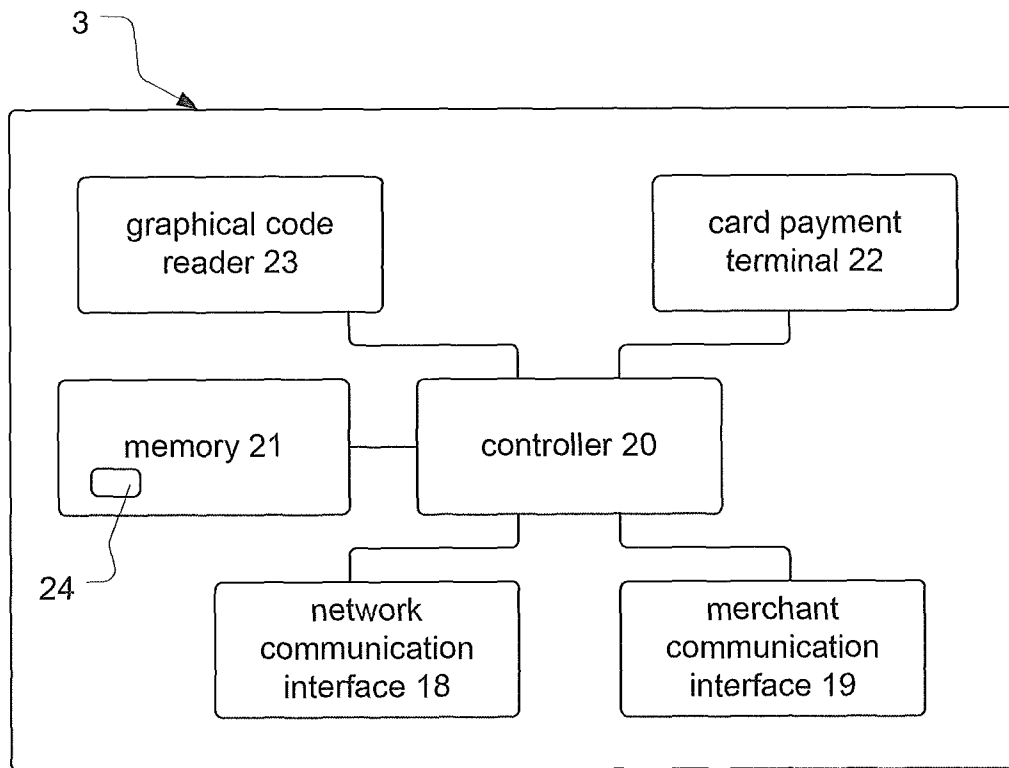


Fig. 3

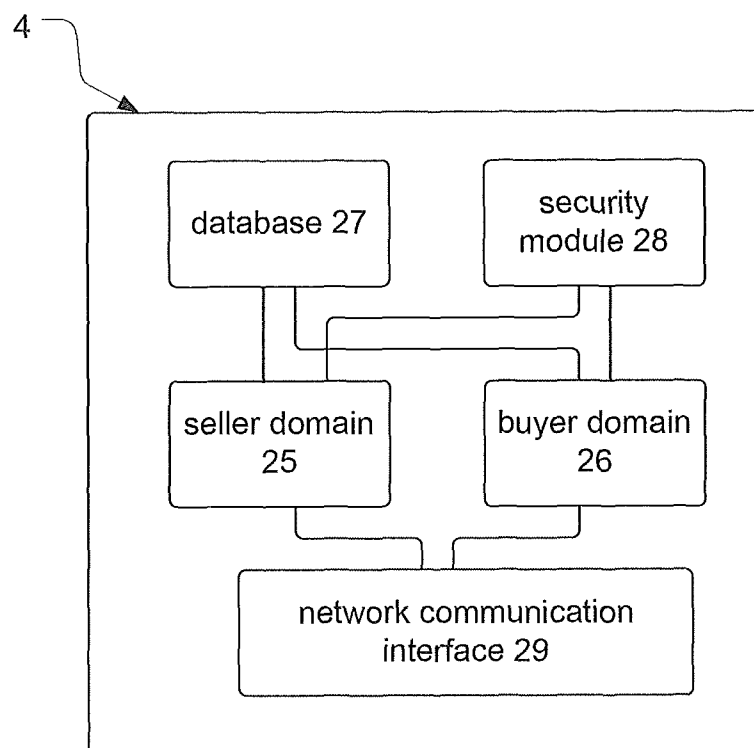


Fig. 4

3/7

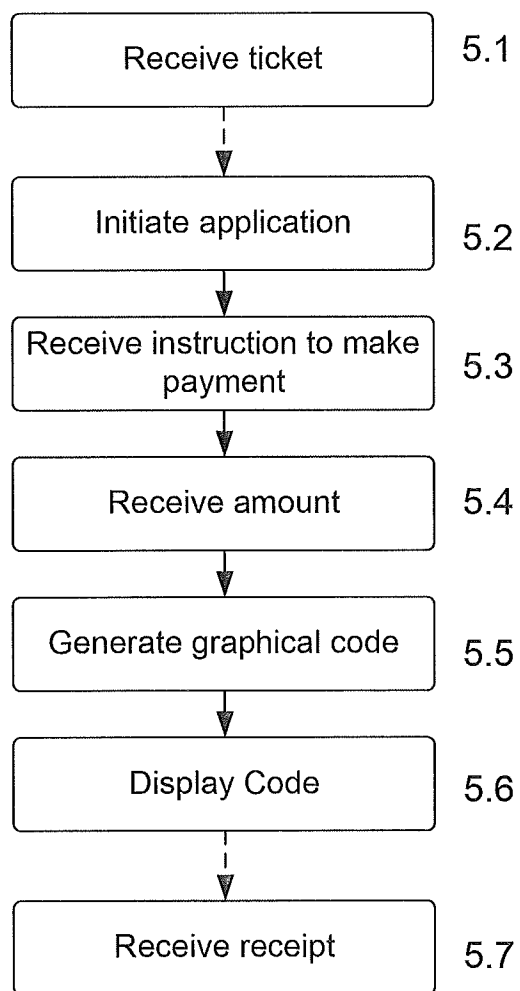


Fig. 5

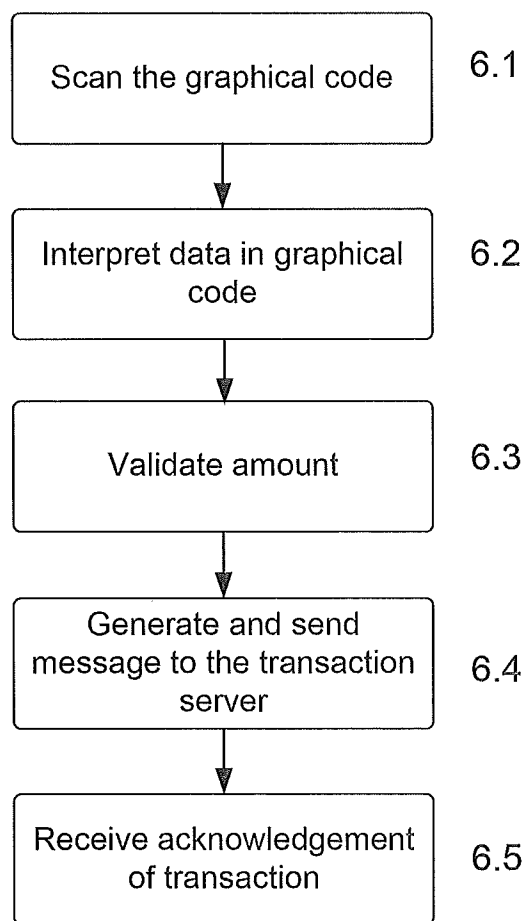


Fig. 6

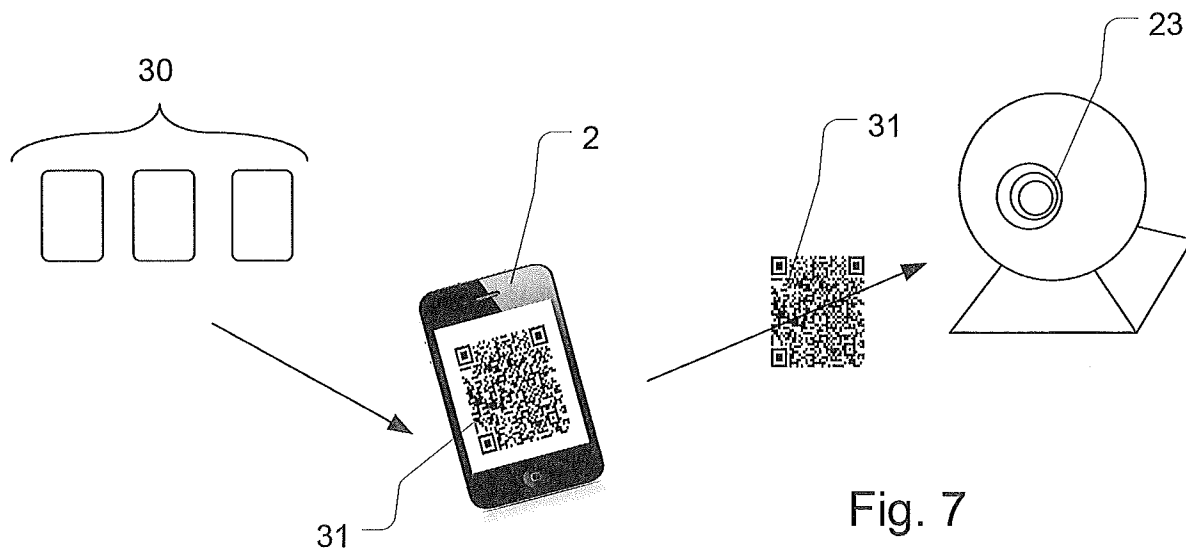
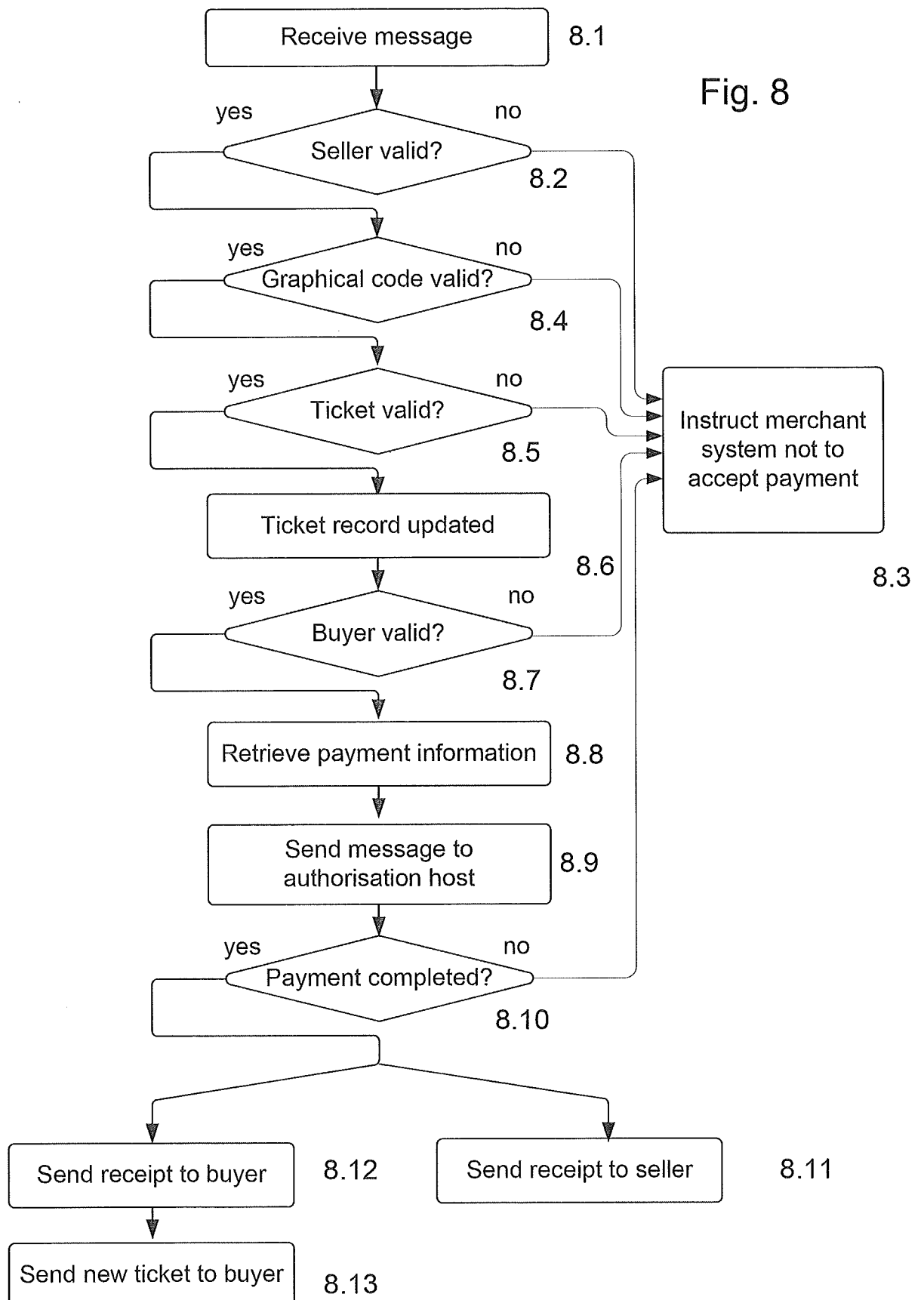


Fig. 7

4/7

Fig. 8



5/7

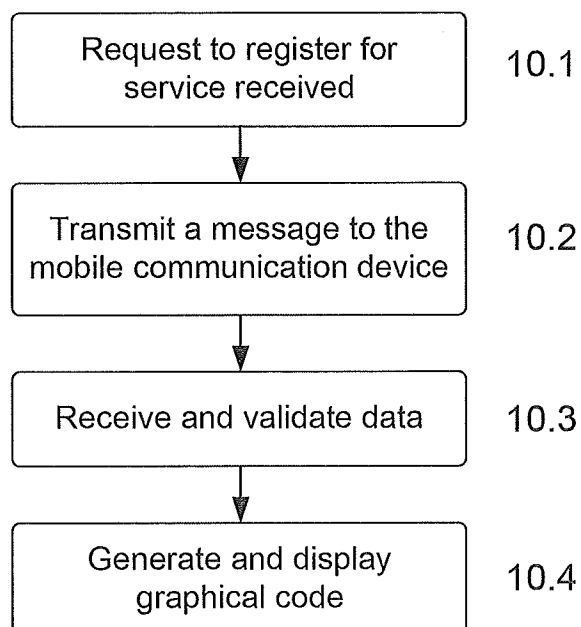
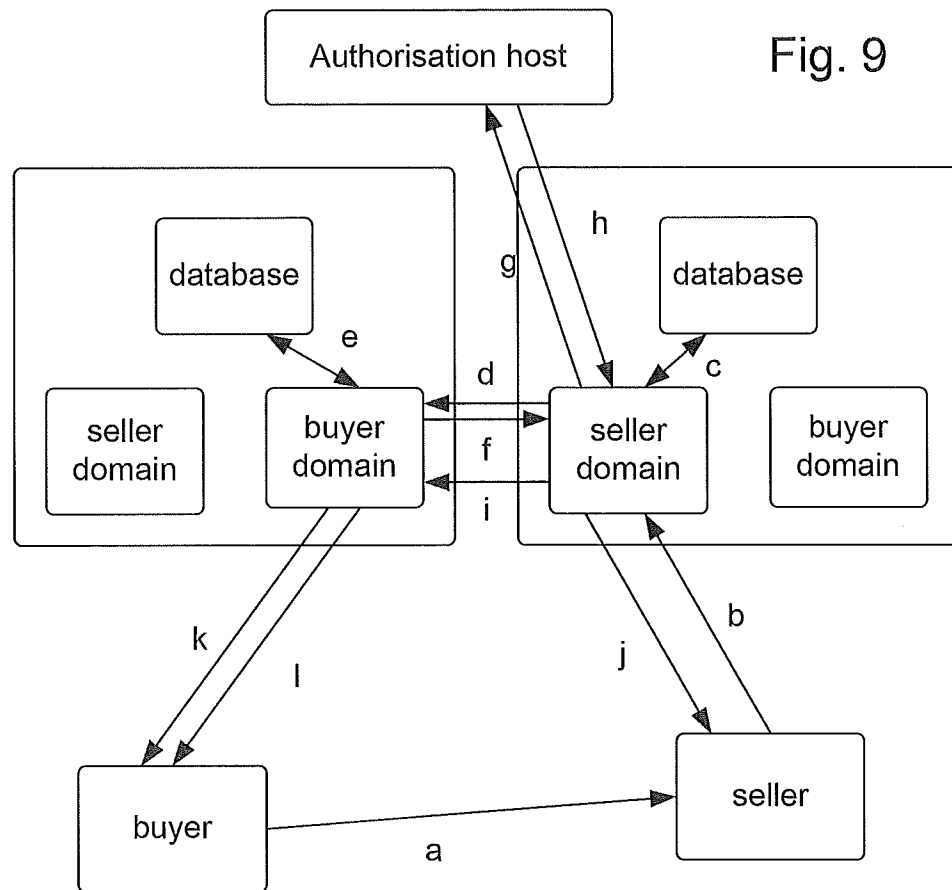


Fig. 10

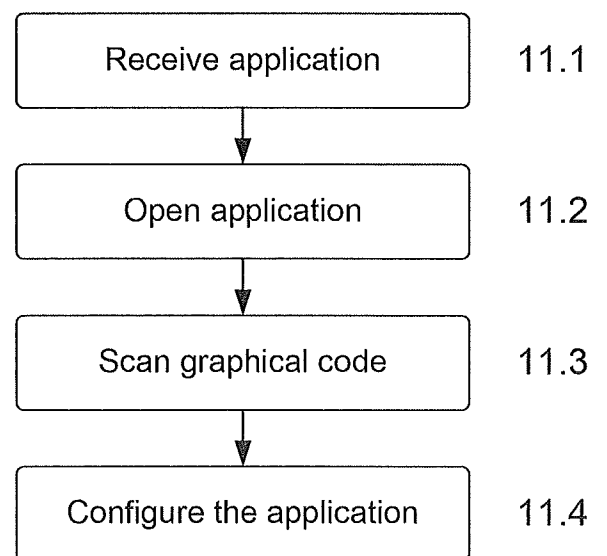


Fig. 11

6/7

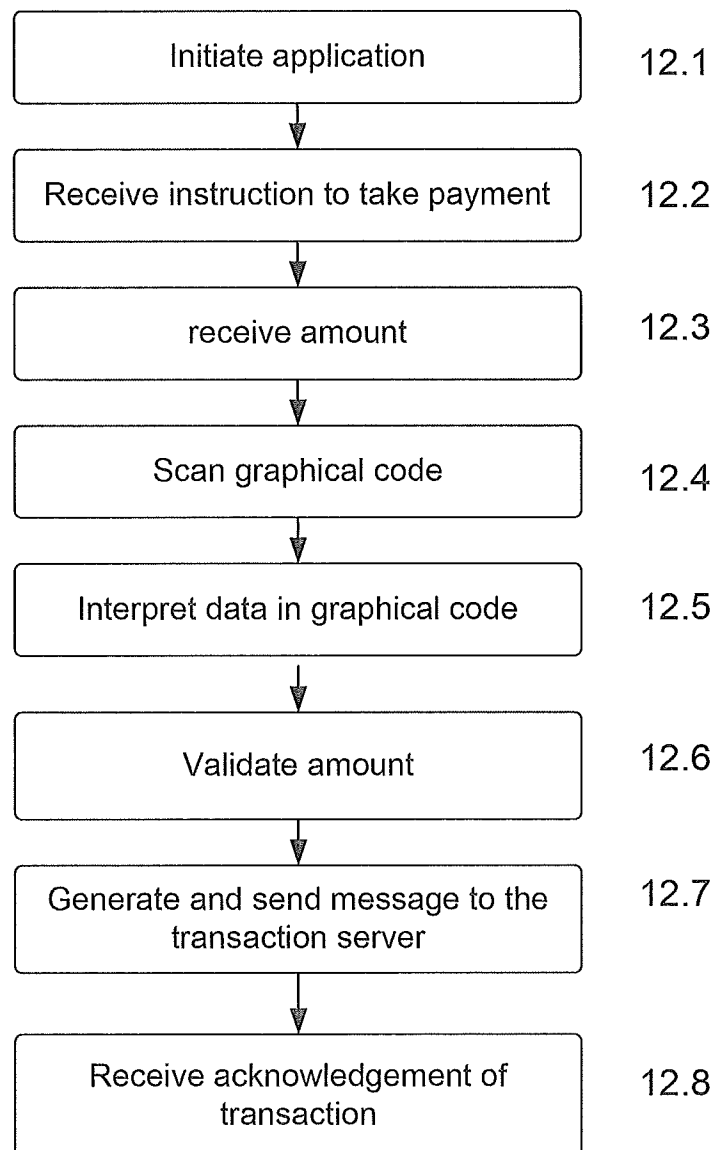
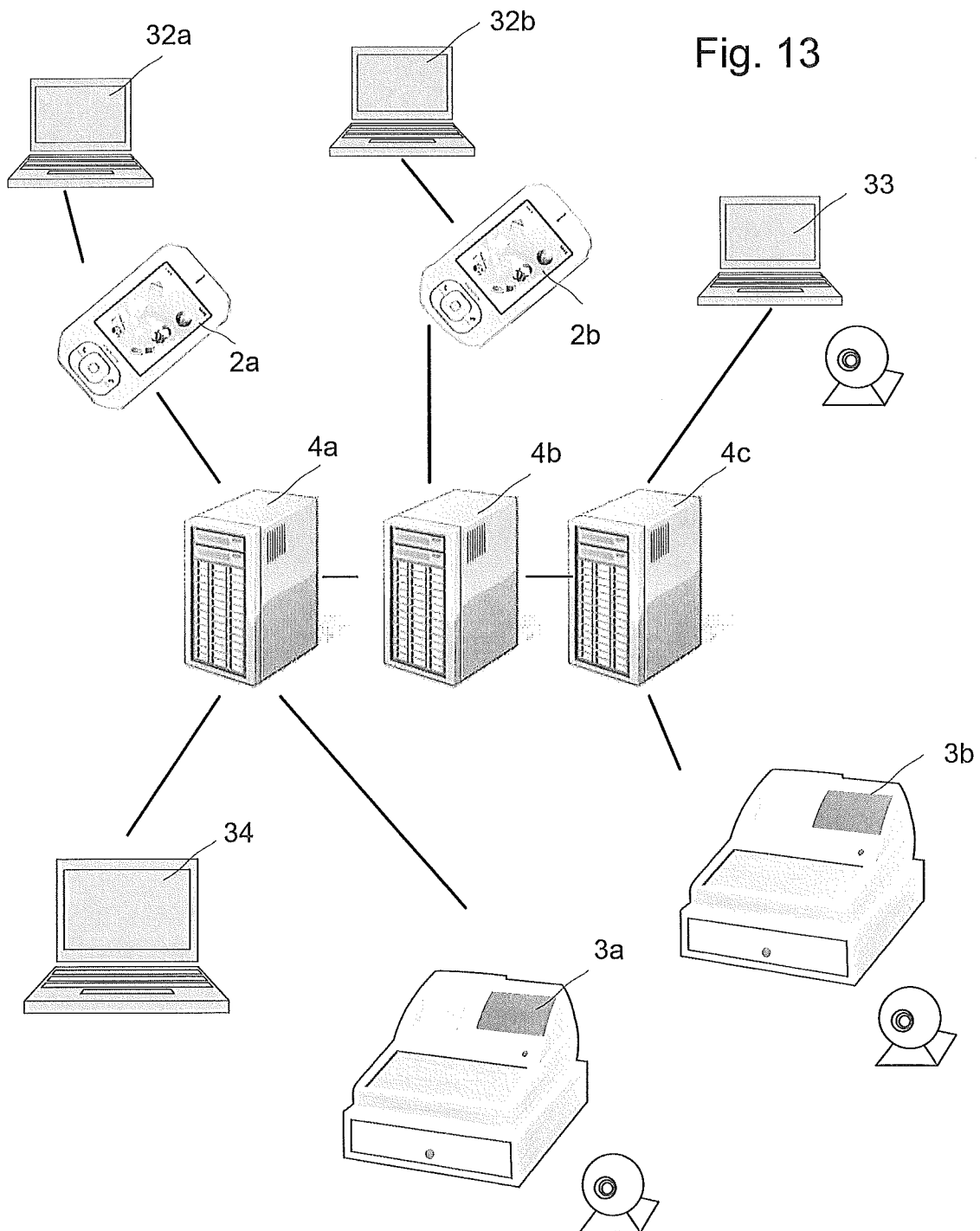


Fig. 12

7/7

Fig. 13



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/060937

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32
ADD.

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008/129828 A1 (CYBERCOIN INC [JP]; NOGUCHI HIROKAZU [JP]) 30 October 2008 (2008-10-30) abstract paragraph [0095] - paragraph [0104] figure 6	1-15
X	WO 2007/117073 A1 (KIM DONG GYU [KR]) 18 October 2007 (2007-10-18) abstract paragraph [0042] - paragraph [0081]	1-15
X	US 2010/125509 A1 (KRANZLEY ARTHUR D [US] ET AL) 20 May 2010 (2010-05-20) abstract paragraph [0019] - paragraph [0034]	1-15
	----- -/-	



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is 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

16 July 2012

Date of mailing of the international search report

25/07/2012

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

Diepstraten, Marc

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/060937

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/008735 A2 (IBREVA CORP [US]; GIORDANO CLAETON J [US]; GREEN DONALD T [US]) 17 January 2008 (2008-01-17) the whole document -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2012/060937

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008129828 A1	30-10-2008	CN 101641707 A	03-02-2010
		JP 2008250884 A	16-10-2008
		WO 2008129828 A1	30-10-2008

WO 2007117073 A1	18-10-2007	NONE	

US 2010125509 A1	20-05-2010	US 2010125509 A1	20-05-2010
		US 2010125516 A1	20-05-2010

WO 2008008735 A2	17-01-2008	US 2008011825 A1	17-01-2008
		WO 2008008735 A2	17-01-2008
