Title: VERIFICATION OF A DATA LINK

Abstract: Communication system comprising a first communication unit and at least a second communication unit, wherein the first communication unit and the at least second communication unit are in communication with one another and are suitable for exchanging signals, wherein the signals comprise text messages and wherein the second communication unit sends a reply message as a response to a first text message sent from the first communication unit to the second communication unit, wherein the reply message from the second communication unit contains a sub-block for authenticity data, from the content of which the first communication unit, after receipt of the reply message, is able to establish whether the reply message is authentic.
Verification of a data link

The invention relates to a communication system according to the precharacterising clause of Claim 1. The invention furthermore relates to a method for a communication system. In addition, the present invention relates to a computer system as a component of the communication system and to a computer program for carrying out the method for the communication system.

The present invention furthermore relates to an automated transaction system.

Such a communication system that comprises at least a first and a second communication unit is known from the state of the art. In the system the at least first and second communication unit can be in communication with one another for exchanging communication signals. Telecommunication systems that make use of fixed and/or wireless links between two or more communication units, that is to say subscribers, have already existed for a long time.

Such telecommunication systems make use of communication signals by means of which various types of data can be transmitted between the subscribers. These signals comprise analogue and/or digital signals and can relate to both the transmission of audio signals and the transmission of symbols, which can be displayed on, for example, a screen of a communication unit.

A communication system that has been known for some time makes use of the sending and receiving of SMS messages. SMS, also termed Short Message Service, is a system that is able to exchange messages in the form of a series of characters between suitable telecommunication units. Telecommunication units suitable for this purpose are, for example, telephones and some handheld computers (personal digital assistants).

The exchange of an SMS message proceeds via a supplier unit (where the message is composed) via a central system to a receiver unit (for which the message is intended). In the first instance the central system comprises the network system of the telecommunications company for the supplier. This network system provides for (temporary) storage of the message and for the transmission thereof to the receiver unit by making use of the telephone number for the receiver's communication unit. The telephone number of his or her handset thus serves for identification of the receiver.

For applications where a response is needed from the receiver it is usually possible for the receiver to be able to send a reply message. Many telecommunication units provide a simple method for replying by automatically putting the number of the original supplier
in a new reply message to be composed by the receiver's telecommunication unit.

The state of the art has the disadvantage that although the reply received by the original supplier can be identified by the telephone number of the original receiver, this cannot provide any guarantee that the reply message has actually been composed by the receiver.

Applications where this can be of importance are, for example, reservations for admission tickets, for events, for travel tickets (such as train or aircraft), placing an order, making a payment or issuing a mandate or authorisation. For these and similar applications a verification of the authenticity of the sender is important.

It is therefore an objective of the present invention to provide a communication system that eliminates the disadvantage in the state of the art and provides a guarantee that the reply message is authentic.

This objective is achieved by a communication system according to the precharacterising clause of Claim 1, characterised in that the second communication unit transmits a reply message as a response to a first text message sent from the first communication unit to the second communication unit, wherein the reply message from the second communication unit contains a sub-block for authenticity data, from the content of which the first communication unit is able, following receipt of the reply message, to establish whether the reply message is authentic.

What is advantageously achieved by this means is that the reply message can be regarded as genuine. The original supplier now knows that the message has actually originated from the receiver.

In addition, it offers the receiver, as a legitimate user of the second communication unit, the advantage that a third party will not be able inadvertently or deliberately to send a reply message in his or her place. This protects the receiver against misuse of his or her telephone and messages sent using this.

The invention also relates to a method for a communication system for exchanging signals, wherein the signals comprise text messages, characterised in that the method comprises the following steps:

- sending a first text message;
- receiving a reply message in response to the text message, wherein the reply message contains a sub-block for authenticity data;
- establishing on the basis of the content of the sub-block for authenticity data whether the
reply message is authentic.

In addition the present invention relates to a processing unit as a component of the communication system, characterised in that the processing unit is equipped to receive a reply message from the second communication unit as a response to a first text message sent to the at least second communication unit, wherein the reply message from the second communication unit contains a sub-block for authenticity data, on the basis of the content of which the processing unit is able to establish whether the reply message is authentic.

Finally, the invention relates to a computer program for carrying out the method for the communication system, characterised in that, after it has been loaded, the computer program product enables the processing unit to perform the following steps:

- sending a first text message;
- receiving a reply message in response to the text message, wherein the reply message contains a sub-block for authenticity data;
- establishing, on the basis of the content of the sub-block for authenticity data, whether the reply message is authentic.

Moreover, the invention relates to an automated transaction system according to the precharacterising clause of Claim 15, characterised in that the processing unit is equipped to perform the following actions:

- monitoring in real time information that has originated from an information source on the network and deciding on the basis of the development of the information monitored to prepare a transaction relating to that information;
- in the case of a decision to prepare a transaction, to send a text message relating to this transaction in preparation to the at least one second communication unit;
- receiving a reply message from the at least one second communication unit;
- establishing the authenticity of the reply message;
- if the reply message is authentic, establishing positive agreement to the transaction in preparation;
- in the case of positive agreement, establishing a share in the transaction for a keeper of the at least one second communication unit, and adding the share to a total for the transaction in preparation;
- composing an instruction for the transaction in preparation and sending the instruction to a dealing system that deals further with the instruction.

The invention also relates to a method for a transaction system according to the
precharacterising clause of Claim 16, characterised in that
the method comprises the following actions:
- monitoring in real time information that has originated from an information source on the
  network and deciding on the basis of the development of the information monitored to
  prepare a transaction relating to that information;
- in the case of a decision to prepare a transaction, to send a text message relating to this
  transaction in preparation to the at least one second communication unit;
- receiving a reply message from the at least one second communication unit;
- establishing the authenticity of the reply message;
- if the reply message is authentic, establishing positive agreement to the transaction in
  preparation;
- in the case of positive agreement, establishing a share in the transaction for a keeper of
  the at least one second communication unit, and adding the share to a total for the
  transaction in preparation;
- composing an instruction for the transaction in preparation and sending the instruction to
  a dealing system that deals further with the instruction.

The invention also relates to a computer program according to the precharacterising
clause of Claim 17, characterised in that
after it has been loaded, the computer program enables the processing unit to perform the
following actions:
- monitoring in real time information that has originated from an information source on the
  network and deciding on the basis of the development of the information monitored to
  prepare a transaction relating to that information;
- in the case of a decision to prepare a transaction, to send a text message relating to this
  transaction in preparation to the at least one second communication unit;
- receiving a reply message from the at least one second communication unit;
- establishing the authenticity of the reply message;
- if the reply message is authentic, establishing positive agreement to the transaction in
  preparation;
- in the case of positive agreement, establishing a share in the transaction for a keeper of
  the at least one second communication unit, and adding the share to a total for the
  transaction in preparation;
- composing an instruction for the transaction in preparation and sending the instruction to
a dealing system that deals further with the instruction.

Finally, the invention relates to a data carrier for a computer program product.

The invention will be explained in more detail below with reference to a few drawings in which illustrative embodiments thereof are shown. They are intended solely as illustration of the aims of the invention and not as a restriction of the inventive concept, which is defined by the appended claims.

In the drawings:

Figure 1 shows, diagrammatically, a telecommunication system according to one embodiment of the present invention;

Figure 2, shows, diagrammatically, a message from a supplier;

Figure 3 shows, diagrammatically, a reply message from a receiver as reply to a message from the supplier according to the present invention;

Figure 4 shows, diagrammatically, a processing unit for processing the reply message according to the present invention;

Figure 5 shows a block diagram for a method for processing the reply message according to the present invention, and

Figure 6 shows a block diagram for a method for a stock transaction system according to the present invention.

Figure 1 shows, diagrammatically, a telecommunication system according to one embodiment of the present invention. In this telecommunication system there is a multiplicity of communication units 1, 2, 3, 4, 6, 7 and 8 that are able to enter into communication with one another. The telecommunication system can comprise both a wireless network system 5a and a fixed (or wired) network system 5b.

The communication units can be mobile communication units 2, 3, 4, such as mobile telephones, and handheld computers or (portable) personal computers that make use of wireless communication links 5a. In the fixed network system 5b the communication units are, for example, fixed telephones with a wire connection to the network and (personal) computers 7. Reference numeral 8 indicates a first communication unit that is suitable for applications according to the present invention.

The fixed network 5b and the wireless network 5a are coupled to one another via a link 5c, where a base station 1 provides the communication with the mobile communication units. It is also conceivable that the network has a further link 9 to other networks.
For the present invention it is important that the network in any event supports the function of sending text messages or SMS messages and that communication units are able to receive and send text messages or SMS messages.

The present invention is implemented in network 5a, 5b outlined above.

The first communication unit 8, which can be mobile or fixed, sends a text message or SMS message to a second communication unit. The first communication unit 8 will be explained in more detail with reference to Figure 4.

For this purpose the identification number of the chosen second communication unit (for example the telephone number or an identification number as node in the network) is sent via the conventional method(s) together with the text message to the network exchange (or a server, not shown). The network exchange establishes a link to the second communication unit 2; 3; 4; 6; 7 by means of the identification number and sends the text message to the second communication unit.

The second communication unit 2; 3; 4; 6; 7 receives the text message.

In the present invention the text message has a content to which the receiver using the second communication unit is provided with an opportunity to respond.

Furthermore it is the case that, if the receiver responds, the response to the text message must be authentic. The supplier of the message via the first communication unit assumes that the second communication unit belongs to a person known to him or her. It must now be possible clearly to establish that the response has actually originated from said known person as receiver and not from a third party who inadvertently or deliberately is faking the response from the receiver.

The user of the second communication unit (the receiver actually intended) can now send a reply message back to the first communication unit of the original supplier.

Figure 2 shows, diagrammatically, a message from a supplier. The message M is shown as a data block that contains at least 3 sub-blocks M1, M2, M3. Subdivision into sub-blocks is known to those skilled in the art from the text message protocol applied.

A first sub-block M1 contains an identification address for the receiver, for example the telephone number of the intended receiver's telephone suitable for text messages. A second sub-block M2 contains address information for the supplier of the message, which information is needed for sending the reply message, i.e. for example, the telephone number to which the reply message has to be sent. In the case of SMS messages this is usually a recognition number or "caller ID" made available by an administrator of the
network 5a, 5b.

Finally, the third sub-block M3 contains message information to which the receiver has to respond in an authentic manner, if desired.

Figure 3 shows, diagrammatically, a reply message from a receiver as reply to a message from the supplier according to the present invention. The reply message R is shown as a data block that contains at least three sub-blocks R1, R2, R3. A first sub-block of the reply message R1 contains an identification address for the receiver (i.e. the reply number for the original supplier as given in the second sub-block M2 of the message. The second sub-block R2 of the reply message R contains address information for the supplier (originally the receiver of message M). In the case of SMS messages this is usually a recognition number or "caller ID" made available by an administrator of the network 5a, 5b.

Finally, the third sub-block R3 of the reply message contains reply information that contains the response to message information M3. Within the third sub-block R3 the reply information contains an authenticity data block R3a, the contents of which can indicate that the reply has indeed originated from the person whose identity the supplier of message M assumes to know.

Authenticity data block R3a preferably contains a personal identification code P that the original receiver has added to the reply message R. The personal identification code P can also be a password if use is made of an alphanumeric keyboard on the second communication unit.

For establishing the correct content of the authenticity data block R3a it can be determined in advance that this doesn’t change or that the content is established again in each case for each message in some way or other. This is dependent on the level of protection and/or security that is desired when establishing the authenticity.

In addition to the recognition number identification of the reply message R offered by the network 5a, 5b by means of second sub-block M2, a further independent identification can now take place by verifying the content of the authenticity data block R3a.

The signal from the reply message R that is sent via the network 5a, 5b thus contains an authenticity signal by means of the authenticity data block R3a.

Figure 4 shows, diagrammatically, a processing unit for processing the reply message according to the present invention.

The first communication unit 8 comprises a processing unit for processing the reply
message, consisting of at least a central processing unit 21 with peripherals. The central processing unit 21 is connected to memory 18, 19, 22, 23, 24, which store instructions and data, one or more readers 30 (to read, for example, floppy disks, CD-ROMs and DVDs, memory cards, etc.), a keyboard 26 and a mouse 27 as input equipment, and, as output equipment, a monitor 28 and a printer 29. Both other input units, such as a track ball, a barcode reader, a scanner and a touch screen, as well as other output equipment can be provided.

The central processing unit 21 is also provided with a network adapter 5d for data communication with the network 5a, 5b. The network adapter 5d is connected to the network 5a, 5b.

The memories shown in Figure 4 comprise RAM 22, (E)EPROM 23, ROM 24, tape unit 19 and hard disk 18. However, more and/or different memory units can be provided, as will be clear to a person skilled in the art. Moreover, if needed, one or more units amongst these can be installed remotely from the central processing unit 21.

The central processing unit 21 is shown as a single unit but can also comprise various processing units that operate in parallel or are controlled by one central unit, it being possible for the processing units to be installed remotely from one another, as will be known to those skilled in the art.

The central processing unit 21 can be part of a communication unit, reply messages R received by the communication unit being passed on to the central processing unit. It is also possible that the central processing unit 21 as such is incorporated in the network 5a, 5b as an independent communication unit and that reply messages R are received directly by the central processing unit 21.

The memory means of the central processing unit 21 contain data relating to authenticity of text messages that preferably are stored in an authenticity database ADB. For each receiver stored therein this authenticity database ADB contains data that at least link the identification number of his or her communication unit with an authenticity characteristic predetermined for the receiver, such as the abovementioned personal identification code.

Figure 5 shows a block diagram for a method for processing the reply message according to the present invention.

In Figure 5 a procedure 100 is shown that can be used for establishing whether a reply message R is authentic.
The procedure starts in step 105 with necessary initialisation by the central
processing unit when a reply message R is received from the network 5a, 5b.

In step 110 the central processing unit 21 reads the received reply message R into the
memory means.

In step 115 the central processing unit 21 divides the reply message R into the at least
three sub-blocks described above, i.e. the first sub-block R1, the second sub-block R2 and
the third sub-block R3 of the reply message R.

In a following step 120 the central processing unit 21 determines the communication
unit from which the message has originated from the second sub-block R2 by means of the
identification number stored in R2.

In a subsequent step 125 the central processing unit 21 retrieves from an authenticity
data bank ADB stored control data CD for the authenticity data block R3a that belongs to
the person to whom the communication unit from which the reply message has originated
belongs.

In step 130 the central processing unit 21 compares information in the control data
CD with the contents of the third sub-block R3 of the received reply message R established
in step 115. A test is performed to determine whether the authenticity data block R3a with
the correct content is indeed present in the third sub-block R3, that is to say that the
message has been authentically sent by the user belonging to the communication unit.

If the test is successful (authenticity data block R3a with the correct content is present
in the message that has been received from the communication unit of the given receiver),
the central processing unit 21 continues in step 140 with processing the remainder of the
message information from third sub-block R3. The content is possibly determined in more
detail by a parser and on the basis of this is further processed by the central processing unit
21. The central processing unit 21 can also, for example, forward the message to an
operator who deals with the message further.

Should the test in step 130 be unsuccessful it is possible that the processing unit
sends a notification of this to the communication unit of the sender of the reply message R.
Wording to the effect that the message was not authentic can be included in the
notification. The notification can also contain wording to the effect that the sender sends
another reply message containing the correct personal identification code in authenticity
data block R3a.

The procedure terminates in step 150.
Searching through the message information in step 130 can take place in various ways. For example, a fixed position of the possible authenticity data block R3a within message information block R3 can be assumed. The position of the personal identification code can also be left free, provided this code is present within reply message information R3. In the latter case it is possible to search for the code of the authenticity data block R3a by means of suitable pattern recognition.

Those skilled in the art will know that procedure 100 for authenticity checking on the basis of an authenticity data block R3a that may or may not be present can be carried out in several alternative ways. The abovementioned procedure serves solely as an example of how the presence and accuracy of the authenticity data block R3a can be established.

It is also pointed out that in step 130 the control data CD can be identical to the authenticity characteristic (or personal identification code) that is in the authenticity data block R3a (when the message is authentic). However, it is also possible that processing of the control data CD together with the content of the authenticity data block R3a by the central processing unit 21 yields a test result that indicates whether or not the reply message R is authentic.

The present invention will be explained in more detail below with reference to a number of embodiments and applications.

Applications in which the authenticity of a reply message can be important usually relate to situations in which the reply message contains confirmation of a proposed transaction. Applications where this can be of importance are, for example, reservations for admission tickets, for events, for travel tickets (such as train or aircraft), placing an order, making a payment or issuing a mandate or authorisation. For these and similar applications verification of the authenticity of the sender is important.

The abovementioned applications assume a customer who makes use of the present invention to purchase a service or product has an identity known to the supplier of the services or products.

In such a case a supplier sends, for example, a message to the customer. The customer sees the message and wishes to respond to this in confirmation. The customer then sends a reply message R containing a personal identification code that is in the authenticity data block R3a.

A preferred embodiment of the invention comprises a stock transaction system.

Figure 6 shows a block diagram of a procedure 200 in a stock transaction system in
which the present invention is employed.

In the stock transaction system in which the present invention can be employed there is an investment company and customers of the latter.

The investment company aims to make a contribution to its customers' assets via buying and selling stocks such as shares and other securities quoted on the stock exchange.

To this end the investment company monitors the prices of relevant stocks over time. This can take place via an automatic instruction system (in step 210). This automatic instruction system is preferably the computer system 8 of the first communication unit that is linked to a network (for example the network 5b) from which the stock price information can be received from an information source such as a server that provides price information. On the basis of the stock price information received, the automatic instruction system 8 can perform a calculation to determine whether there is a change in price that can produce a favourable transaction. At the point in time when an opportunity arises for a purchase that can have an advantageous result within the strategy of the investment company, the envisaged customers, that is to say customers for whom this can be relevant, are contacted (by telephone). (In practice this can also be done for sell transactions, but usually this is not necessary because what can be an advantageous sale can be established in advance by consultation). In such a case each envisaged customer is informed of the possible advantageous buy transaction that can be performed. If the customer wishes to participate with a share in the buy transaction, he or she will have to confirm this during the contact.

Contacting each of the customers individually and collecting participations in this way, however, takes too long and is too complex because in some cases the opportunities for an advantageous buy transaction can be within a relatively very short time, shorter than the time needed to inform all envisaged customers.

Therefore, in such a case provision is made to contact all envisaged customers at the same time sending a text message via the telecommunication system according to the present invention. Moreover, this advantageously removes possible inequality between customers who otherwise would be approached via a telephone call in a certain order in time.

So as to be able to be in contact with the first communication unit 8 of the investment company, each envisaged customer K is provided with a second communication unit 2; 3; 4; 6; 7 that is able to receive a text message M and that is able to send a reply message R.
Such a second communication unit is, for example, the mobile telephone or other device that is able to receive and send text messages, as has already been explained in Figure 1.

In part 220 of the procedure the first communication unit 8 sends a text message M, in which the message information M3 contains an indication of the possible transaction, via the network 5a, 5b.

Each envisaged customer K receives the text message M, where the message information M3 is visible, via his or her respective second communication unit 2; 3; 4; 6; 8 (sic).

If the customer K wishes to participate in the possible transaction, he or she must send a reply message R to the first communication unit 8.

For this purpose the customer K composes a reply that is included in the reply message information R3 of the reply message R.

In order to confirm that it is actually the customer K who is confirming his or her participation and not a third party who inadvertently or deliberately has the customer's communication unit in his or her possession, the customer must at this point add a personal identification code P to the message information R3 in the reply in the form of an authenticity data block R3a. The customer has previously agreed this personal identification code P with the investment company. In the first communication unit 8 this personal identification code is stored in an authenticity database ADB in the memory 18, 19, 22, 23, 24 of the first communication unit 8.

After compiling the reply message R, the customer K sends the message to the reply address that preferably is already known from the address information M2 in the text message M.

In part 230 of the procedure the first communication unit 8 then receives a reply message R from every customer K who wishes to participate. The first communication unit 8 is equipped for processing a received reply message, as has been described above with reference to Figures 4 and 5.

As indicated in procedure 100 in Figure 5, the first communication unit 8 thus checks each received message in the manner mentioned in the case of Figure 5.

Via the second sub-block R2 of the reply message R it establishes from which customer's communication unit the reply message R originated.

The automatic instruction system/first communication unit 8 then checks whether the received reply message is authentic via the information in the authenticity data block R3a.
in the reply message information R3, which is compared with the known personal identification code that has been stored in the authenticity database ADB. The presence of the personal identification code P is tested by the processing unit 21 of the automatic instruction system/first communication unit 8.

Finally, if the reply message is authentic, the reply message information R3 in the reply message R is analysed. In this context analysis denotes: a search to determine whether the reply message contains positive confirmation.

If the message proves not to be authentic, a notification is optionally sent to the sender of the message that the personal identification code is missing in his or her message and that the sender can send the message again in the correct form.

The check for authenticity is carried out by the automatic instruction system for each reply message R received.

The automatic instruction system will then provide for further execution. This execution can take place in various ways, but in any event in part 240 of the procedure comprises establishing customers K who wish to participate in the buy transaction by sending a reply message as confirmation. The details of customers who wish to participate are stored in the memory 18, 19, 22, 23, 24 of the first communication unit 8.

Preferably, in a subsequent part 250 of the procedure the automatic instruction system determines the sum for which customers who replied in the affirmative can participate in the transaction. This can be calculated, for example, from a predetermined funds limit VL (i.e. a maximum participation sum or percentage of available funds CLV) and/or a predetermined risk profile RP (i.e. an indication that indicates a participation limit depending on the type of transaction). Such data VL, CLV, RP are, for example, stored in a contract database CDB for each customer K. The automatic instruction system reads these data from contract database CDB (255) stored in memory 18, 19, 22, 23, 24 of the first communication unit 8. Such a contract database CDB can be linked to the authenticity database ADB.

In part 260 of the procedure the communication unit 8/automatic instruction system can then, for example, establish a total sum for which the buy transaction can be performed (optionally with rounding to whole numbers of securities). In this case the total sum is the sum of the sums from the individual customers who wish to participate.

In part 270 of the procedure a final verification of the quality of the transaction can then also take place: is the envisaged buy transaction still a transaction that is advantageous
within the strategy at this point in the processing operation?

If so, in part 280 of the procedure the automatic instruction system will then be able (after possible authorisation by an authorised person in a preceding part of the procedure or at this point in time within procedure 200) to transmit the instruction to the dealing system in which the transaction has to be performed, for example the (electronic) system of a bank or a stock exchange.

As has already been described above, the passage of time plays an important role in this application, because stock prices and movements can be subject to continual change. Therefore, in a preferred embodiment of the application a time interval for a closing time limit within which a customer must respond will also be used as a process criterion.

In this case the text message M from the first communication unit 8 to the envisaged customers contains an indication of the period within which the customer has to respond. Participation is no longer possible after the closing time limit for the envisaged buy transaction.

If a closing time limit is used, the first communication unit 8 can, in part 230 of the procedure, also fixed on receipt of a reply message R whether the reply message has still been received before the set closing time limit. If the receipt of the reply message R from a customer is before the closing time limit, the customer participates in the transaction and otherwise does not. Optionally, the first communication unit 8 can notify the customer concerned that his or her reply message R arrived too late.

After expiry of the closing time limit the first communication unit 8 will then proceed in part 240 of the procedure with further execution of the envisaged buy transaction, as has already been described above.

Incidentally, it is also conceivable that the time aspect is less important and that a certain (maximum) total sum is taken as process criterion for implementation (within a certain time limit). A person skilled in the art will be aware of the application of such alternative process criteria. In this case the procedure 200 can make provision that after the desired total sum has been reached in part 260 of the procedure further reply messages that have not yet been processed will not be dealt with.

The first communication unit 8 is equipped to store received reply messages R in its memory 18, 19, 22, 23, 24 and to store (intermediate) results of processing operations as shown in Figure 5 and Figure 6. An indication of the time of receipt can be included for each received reply message R in the memories 18, 19, 22, 23, 24.
The first communication unit 8 can also display (to an operator) the progress of processing operations and the status thereof, for example the number of positive reply messages received, incorrect messages, non-authentic messages, and also what total sum is available for the envisaged buy transaction.

The automatic instruction system can also provide for notification concerning transmittal of the buy transaction to the dealing system concerned.

Finally, the first communication unit 8 can provide a facility for informing the participating customers K after the transaction has been performed of the individual details relating to them, such as their individual participation sum in the transaction, as can be calculated from the available funds CLV, the funds limit for participating VL and the risk profile RP. A total list of all outstanding participations for a particular customer can also be reported in this notification.

Other alternatives and equivalent embodiments of the present invention are conceivable within the inventive concept, as will be clear to a person skilled in the art. The inventive concept is restricted only by the appended claims.
Claims

1. Communication system comprising a first communication unit (8) and at least a second communication unit (2, 3, 4, 6, 7), wherein the first communication unit (8) and the at least second communication unit (2, 3, 4, 6, 7) are in communication with one another in a network (5a, 5b) suitable for exchanging signals, wherein the signals comprise text messages, characterised in that the second communication unit (2, 3, 4, 6, 7) transmits a reply message (R) as a response to a first text message (M) sent from the first communication unit (8) to the second communication unit (2, 3, 4, 6, 7), wherein the reply message (R) from the second communication unit (2, 3, 4, 6, 7) contains a sub-block for authenticity data (R3a), from the content (P) of which the first communication unit (8) is able, following receipt of the reply message (R), to establish whether the reply message (R) is authentic.

2. Communication system according to Claim 1, characterised in that the first communication unit (8) has a processing unit (21) connected to memory means (18, 19, 22, 23, 24), wherein the processing unit (21) is equipped to establish whether the reply message (R) is authentic.

3. Communication system according to Claim 2, characterised in that the first communication unit (8) for establishing whether the reply message (R) is authentic compares the content of the authenticity data (R3a) with control data (CD) previously stored in a memory bank (ADB) in the memory means (18, 19, 22, 23, 24).

4. Communication system according to Claim 2, characterised in that in the memory bank (ADB) the control data (CD) for the at least second communication unit is linked to a network identification number of the at least second communication unit in a sub-block (R2) of the reply message (R).

5. Communication system according to one of the preceding claims, characterised in that the first or at least second communication units for receiving and sending text messages comprise suitable telephones or personal digital assistants.

6. Communication system according to one of the preceding claims, characterised in that the first communication unit (8) comprises a computer system (21; 18, 19, 22, 23, 24) suitable for receiving and sending text messages.

7. Communication system according to one of the preceding claims, characterised in that the sub-block for authenticity data (R3a) is inside a message information block.
8. Communication system according to one of the preceding Claims 2 - 7, characterised in that the processing unit (21) of the first communication unit (8) is equipped to perform the following actions:

- (210): monitoring in real time information (info) that has originated from an information source on the network (5a, 5b) and deciding on the basis of the development of the information monitored to prepare a transaction relating to that information;

- (220): in the case of a decision to prepare a transaction, to send a text message (M) relating to this transaction in preparation to the at least one second communication unit (2, 3, 4, 6, 7);

- (230): receiving an reply message (R) from the at least one second communication unit (2, 3, 4, 6, 7);

- (100): establishing the authenticity of the reply message (R);

- (240): if the reply message (R) is authentic, establishing positive agreement to the transaction in preparation;

- (250): in the case of positive agreement, establishing a share in the transaction for the keeper (K) of the at least one second communication unit (2, 3, 4, 6, 7), and adding the share to a total for the transaction in preparation;

- (260, 270): composing an instruction for the transaction in preparation and sending the instruction to a dealing system that deals further with the instruction.

9. Communication unit suitable for exchanging signals with an at least second communication unit, wherein the signals comprise text messages, characterised in that the communication unit is equipped to receive a reply message (R) from the second communication unit as response to a first text message (M) from the communication unit sent to the second communication unit, wherein the reply message (R) from the second communication unit contains a sub-block for authenticity data (R3a) from the content of which the communication unit is able to establish whether the reply message (R) is authentic.

10. Processing unit (21) of a first communication unit (8) containing memory means (18, 19, 22, 23, 24), wherein the processing unit (21) is linked to the memory means (18, 19, 22, 23, 24), the first communication unit (8) suitable for exchanging signals with an at least second communication unit, wherein the signals comprise text messages,
characterised in that the processing unit (21) is equipped to receive a reply message (R) from the second communication unit as response to a first text message (M) sent to the at least second communication unit, wherein the reply message (R) from the second communication unit contains a sub-block for authenticity data (R3a), from the content of which the processing unit (21) is able to establish whether the reply message (R) is authentic.

11. Method for a communication system for exchanging signals, wherein the signals comprise text messages, characterised in that the method comprises the following parts:

- sending a first text message (M);
- receiving a reply message (R) in response to the text message (M), wherein the reply message (R) contains a sub-block for authenticity data (R3a);
- establishing on the basis of the content of the sub-block for authenticity data (R3a) whether the reply message (R) is authentic.

12. Method for a first communication unit (8) suitable for exchanging signals with an at least second communication unit, wherein the signals comprise text messages, characterised in that the method comprises the following steps:

- sending a first text message (M);
- receiving a reply message (R) in response to the text message (M), wherein the reply message (R) contains a sub-block for authenticity data (R3a);
- establishing on the basis of the content of the sub-block for authenticity data (R3a) whether the reply message (R) is authentic.

13. Method for a processing unit (21) of a first communication unit (8) containing memory means (18, 19, 22, 23, 24), wherein the processing unit (21) is linked to the memory means (18, 19, 22, 23, 24), the first communication unit suitable for exchanging signals with an at least second communication unit, wherein the signals comprise text messages, characterised in that the method comprises the following steps:

- sending a first text message (M);
- receiving a reply message (R) in response to the text message (M), wherein the reply message (R) contains a sub-block for authenticity data (R3a);
- establishing on the basis of the content of the sub-block for authenticity data (R3a) whether the reply message (R) is authentic.
14. Computer program product for loading by a processing unit (21) of a first
communication unit (8) containing memory means (18, 19, 22, 23, 24), wherein the
processing unit (21) is linked to the memory means (18, 19, 22, 23, 24), the first
communication unit suitable for exchanging signals with an at least second
communication unit, wherein the signals comprise text messages, characterised in
that, after it has been loaded, the computer program product enables the processing
unit (21) to perform the following steps:
- sending a first text message (M);
- receiving a reply message (R) in response to the text message (M), wherein the
reply message (R) contains a sub-block for authenticity data (R3a);
- establishing, on the basis of the content of the sub-block for authenticity data (R3a),
whether the reply message (R) is authentic.

15. Transaction system comprising a first communication unit (8) and at least a second
communication unit (2, 3, 4, 6, 7), wherein the first communication unit (8) and the
at least second communication unit (2, 3, 4, 6, 7) are in communication with one
another in a network (5a, 5b) and are suitable for exchanging signals, wherein the
signals comprise text messages, wherein the first communication unit (8) comprises a
processing unit (21) and memory (18, 19, 22, 23, 24), wherein the processing unit
(21) is linked to the memory (18, 19, 22, 23, 24)

characterised in that
the processing unit (21) is equipped to perform the following actions:
- (210): monitoring in real time information (info) that has originated from an
information source on the network (5a, 5b) and deciding on the basis of the
development of the information monitored to prepare a transaction relating to that
information;
- (220): in the case of a decision to prepare a transaction, to send a text message (M)
relating to this transaction in preparation to the at least one second communication
unit (2, 3, 4, 6, 7);
- (230): receiving a reply message (R) from the at least one second communication
unit (2, 3, 4, 6, 7);
- (100): establishing the authenticity of the reply message (R);
- (240): if the reply message (R) is authentic, establishing positive agreement to the
transaction in preparation;
- (250): in the case of positive agreement, establishing a share in the transaction for the keeper (K) of the at least one second communication unit (2, 3, 4, 6, 7), and adding the share to a total for the transaction in preparation;
- (260, 270): composing an instruction for the transaction in preparation and sending the instruction to a dealing system that deals further with the instruction.

16. Method for a transaction system comprising a first communication unit (8) and at least a second communication unit (2, 3, 4, 6, 7), wherein the first communication unit (8) and the at least second communication unit (2, 3, 4, 6, 7) are in communication with one another in a network (5a, 5b) and are suitable for exchanging signals, wherein the signals comprise text messages, wherein the first communication unit (8) comprises a processing unit (21) and memory (18, 19, 22, 23, 24), characterised in that the method comprises the following actions:
- (210): monitoring in real time information (info) that has originated from an information source on the network (5a, 5b) and deciding on the basis of the development of the information monitored to prepare a transaction relating to that information;
- (220): in the case of a decision to prepare a transaction, to send a text message (M) relating to this transaction in preparation to the at least one second communication unit (2, 3, 4, 6, 7);
- (230): receiving a reply message (R) from the at least one second communication unit (2, 3, 4, 6, 7);
- (100): establishing the authenticity of the reply message (R);
- (240): if the reply message (R) is authentic, establishing positive agreement to the transaction in preparation;
- (250): in the case of positive agreement, establishing a share in the transaction for the keeper (K) of the at least one second communication unit (2, 3, 4, 6, 7), and adding the share to a total for the transaction in preparation;
- (260, 270): composing an instruction for the transaction in preparation and sending the instruction to a dealing system that deals further with the instruction.

17. Computer program product for a transaction system comprising a first communication unit (8) and at least a second communication unit (2, 3, 4, 6, 7), wherein the first communication unit (8) and the at least second communication unit
(2, 3, 4, 6, 7) are in communication with one another in a network (5a, 5b) and are suitable for exchanging signals, wherein the signals comprise text messages, wherein the first communication unit (8) comprises a processing unit (21) and memory (18, 19, 22, 23, 24), wherein the processing unit (21) is linked to the memory means (18, 19, 22, 23, 24), the communication unit [lacuna] suitable for exchanging signals with an at least second communication unit, wherein the signals comprise text messages, the computer program product having to be loaded by the processing unit (21), characterised in that after having been loaded, the computer program product enables the processing unit (21) to perform the following actions:

- (210): monitoring in real time information (info) that has originated from an information source on the network (5a, 5b) and deciding on the basis of the development of the information monitored to prepare a transaction relating to that information;

- (220): in the case of a decision to prepare a transaction, to send a text message (M) relating to this transaction in preparation to the at least one second communication unit (2, 3, 4, 6, 7);

- (230): receiving a reply message (R) from the at least one second communication unit (2, 3, 4, 6, 7);

- (100): establishing the authenticity of the reply message (R);

- (240): if the reply message (R) is authentic, establishing positive agreement to the transaction in preparation;

- (250): in the case of positive agreement, establishing a share in the transaction for the keeper (K) of the at least one second communication unit (2, 3, 4, 6, 7), and adding the share to a total for the transaction in preparation;

- (260, 270): composing an instruction for the transaction in preparation and sending the instruction to a dealing system that deals further with the instruction.

18. Data carrier for a computer program product according to Claim 13 or 17.