(51) International Patent Classification: H04L 29/00

(21) International Application Number: PCT/EP02/06015

(22) International Filing Date: 31 May 2002 (31.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: M2001A001173 1 June 2001 (01.06.2001) IT

(72) Inventor: PURICELLI, Guido [IT/IT]; Via san Calimero, 7, I-20122 Milano (IT).

Inventor and
Inventor/Applicant (for US only): DORNINI, Fabio, Giuseppe [IT/IT]; Via Lorenzo Perosi, 5, I-20146 Milano (IT).

(84) Designated States (regional): ARIPI patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BE, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(74) Agent: PFAU, Anton; Grünbeck, Kinkeldey, Stockmair & Schwanhäusser, Maximilianstrasse 58, 80538 München (DE).


(54) Title: IMPROVING SECURITY IN DATA COMMUNICATION NETWORKS

(57) Abstract: A method and a system for transmitting data over a communication network (3). At least three computer systems (2, 5, 16) are connected to the communication network (3). A first message (7) is sent from the first computer system (2) to the second computer system (5). A second message is sent from the second computer system (2) to the third computer system (16). The third computer systems compares the contents of the second and third messages received from the first and second computer systems and verify the identifies of the subjects who operates the first and second computer systems thus guarantying the identity of the subjects, the confidentiality of the data transmitted and the reliability of the transmission.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
IMPROVING SECURITY IN DATA COMMUNICATION NETWORKS

FIELD OF THE PRESENT INVENTION

The present invention relates to the field of data communication technology; in particular, the present invention relates to a method and a system for communicating and transmitting data over a communication network such as the public switchboard telephone network, cellular phone systems, the internet, or an intranet, etc, allowing to improve the security and the reliability of the transmission. The method and the system according to the present invention finds useful application in the field of commercial transactions; in particular, the method of the present invention can be used for buying and/or ordering goods and/or services in a reliable manner over the internet. The present application also relates to a system for carrying out such a method.

DESCRIPTION OF THE PRIOR ART

In recent years, the transmission of data by means of computer systems connected to a communication network has increased significantly and data are nowadays commonly transmitted over the communication network for several purposes. For instance, e-mail messages are daily sent and received to and from millions of users and users constantly retrieve information from internet web sites. It is also becoming more and more usual to use the internet for executing commercial transactions.

The most common commercial transactions for ordering goods and/or services usually carried out on the public communication networks comprise the following steps: first, a merchant displays the goods for sale, e.g., on a web page. Second, a customer orders the goods, for instance by sending a message to the web site address of the merchant. Once the message has been received by the merchant, the customer is requested to communicate the number of his credit card; if the credit card is revealed to be valid, the order is confirmed and the transfer of money from the customer's account to the merchant's account is carried out.

This technique of executing commercial transactions by using a credit card has several drawbacks. First, it is only possible to verify that the credit card is valid, but there is no
possibility of verifying that the person who has communicated the number of the credit card actually corresponds to the owner of the credit card. Accordingly, anyone who gains knowledge of the number of the credit card is potentially capable of ordering and/or buying goods and/or services from one or more web sites of corresponding merchants under a false name and charging the respective amount on the credit card of the legal owner. This can be, in particular, carried out by anyone intercepting the data relating to the credit card on the communication network as well as by the manager of the web site of the merchant; for instance, managers of the web sites of the merchants could modify the amount corresponding to the transactions disposed by the legal owner of the credit card or the data intercepted could be used for transferring amounts relating to fictitious transactions. Finally, the data intercepted could be communicated to third parties for illegal purposes.

A second disadvantage of the technique of executing commercial transactions according to the prior art relates to the fact that the user is not able to verify whether the web site really corresponds to a merchant who is in a position to furnish the offered goods and/or services.

A further drawback of the technique of executing commercial transactions according to the prior art relate to the fact that the confidential data relating to both the owner of the credit card and the completed order have to be communicated over the communication network; it cannot therefore be excluded that, in spite of all security measures taken, data can be intercepted and misused. In particular, this is the reason why, at present, it is sometimes inconvenient to use a credit card for executing commercial transactions via the internet.

Many efforts have been made in the art for overcoming the above-explained disadvantages and, correspondingly, several transaction methods have been developed and proposed; for instance, so-called S.E.T. (Secure Electronic Transaction) methods have been proposed, according to which the confidential data are encoded and decoded in an attempt of guarantying the identity of those involved in a transaction and the confidentiality of the data transmitted. However, these methods are rather complicated and expensive and the level of security obtained is mostly not satisfying.
Accordingly, in view of the problems explained above, it would be desirable to provide a technique that may be used e.g. for executing commercial transactions over a communication network, thereby solving or at least reducing one or more of these problems.

SUMMARY OF THE INVENTION

According to a first embodiment of the present invention as claimed in claim 1, this is achieved by providing an improved method of transmitting data over a communication network to which at least three computer systems are connected, wherein said method comprises sending a first message from a first one of said at least three computer systems to a second one of said at least three computer systems, with said first message containing at least a first code and data. Additionally, the inventive method comprises sending a second message from the second computer system to at least one of the at least three computer systems, with said second message containing a second code as well as the first code and the data. Furthermore, the method comprises sending a third message from the first computer system to the third computer system, with said third message containing a third code as well as encoded data containing the second code and the data. Moreover, according to the method of the present invention, the third computer system performs the steps of: decoding the encoded data to extract the second code and the data from the encoded data; generating a fourth code on the basis of the third code; comparing the extracted data with the data contained in the second message; comparing the extracted code with the second code contained in the second message; comparing the fourth code with the first code contained in the second message.

According to another aspect of the present invention as claimed in claim 14 there is further provided a system for transmitting data over a computer network, wherein said system comprises at least a first computer system, a second computer system and a third computer system adapted to be connected to the communication network, with said at least first computer system being adapted to send at least a first message to at least the second computer system, with said first message containing at least a first code and additional data. Moreover, according to the inventive system, said at least second computer system is adapted to send at least a second message to the third computer system, with said second message containing a second code as well as the first code and the additional data. Furthermore, according to the system of the present invention, said
at least first computer system is adapted to send at least a third message to the at least third computer system, with said third message containing a third code as well as encoded data containing the second code and the additional data. Additionally, said at least third computer system comprises means for performing the following steps: decoding the encoded data to extract the second code and the additional data; generating a fourth code on the basis of the third code; comparing the extracted data with the additional data contained in the second message; comparing the extracted code with the second code contained in the second message; comparing the fourth code with the first code contained in the second message.

According to a still preferred embodiment of the present invention as claimed in claim 25 there is provided a system for transmitting data over a computer network, with said system comprising at least a first computer system and a second computer system both adapted to be connected to the communication network, wherein said at least first computer system is adapted to send at least a first message to the at least second computer system, with said first message containing a first code as well as encoded data containing a second code and additional data. Moreover, according to the system of the this preferred embodiment of the present invention, said at least second computer system comprising means for performing the following steps: decoding the encoded data to extract the second code and the additional data from the encoded data; generating a third code on the basis of the first code; comparing the extracted additional data with corresponding data contained in a second message; comparing the extracted code with a corresponding code contained in the second message; comparing the third code with a corresponding code contained in the second message.

Further preferred embodiments of the present invention are defined in the appended dependent claims.

The method according to the present invention is based on the following concepts.

The user and the merchant communicate on a specific channel by using predefined codes (a first code identifying the user and, optionally, a second code identifying the merchant).
The user and the account manager communicate on another specific channel and the user transmits to the account manager a third code identifying the user as well as encoded data containing the second code identifying the merchant and data relating to the order. The encoded data are encoded by the user according to a predefined encoding key. Correspondingly, the encoded data are decode by the account manager according to a predefined decoding key assigned to the encoding key used by the user.

The merchant and the account manager communicate on still another specific channel and the merchant transmits to the account manager the first code identifying the user, the second code identifying the merchant and the data relating to the order.

The account manager decodes the encoded data received by the user and generates a fourth code identifying the user on the basis of the third code identifying the user. By decoding the encoded data, comparing the fourth generated code identifying the user with the code identifying the user as submitted by the merchant and comparing the data contained in the messages received by the user and the merchant, the account manager verifies the identity of both the user and the merchant as well as the data relating to the order. Only once the identity of the subjects of the transactions has been verified, the order is executed and the transfer of the corresponding amount from the account of the user to the account of the merchant is disposed.

By preventing unauthorized subjects from gaining access to the confidential data of the user and by avoiding manipulation of the data relating to the order specified in the transaction, the method and the system according to the present invention allow the avoidance of any interference by unauthorized subjects as well as any other manipulation. In case of manipulation and/or unauthorized interference, the transaction is stopped.

The messages sent during a transaction executed according to the method of the present invention are at least partially encoded and none of said messages contain the entire data relating to the order and the identity of the subjects involved in the transaction.

Accordingly, in order to be able to execute an unauthorized transaction, a fraudulent person would first have to execute the following operations:
- steal the user's credit card or intercept the number of the credit card over the Internet; (when another card is used, for instance a card specially delivered to users who intend to use the present method, said special card or even another similar document should be stolen)
- steal the list of the encoding keys used for encoding the data contained in the message sent from the user to the account manager as well as the code identifying said list;
- violate, via the communication network, the server of the account manager so as to obtain the copies of the encoding and decoding keys assigned to the user;
- steal the code identifying the user;
- send to the account manager over the communication network the data relating to the fictional transaction and firstly assume the identity of the user and then that of the merchant.
- to be a real merchant; in fact, if the identifying code transmitted to the account manager does not correspond to that of an authorized merchant the account manager prevents any transfer of money.

As a result, it is highly unlikely that all of these operations could be carried out.

Furthermore, according to a preferred embodiment of the method of the present invention, once the transaction has been executed, the encoding keys used by the user are deactivated and can no longer be used.

Fraud on the part of the merchant is also avoided since the account manager does not confirm transfers of amounts other than those indicated by the user. Moreover, by means of the code identifying the merchant, the user could recognize the identity of a merchant who manipulates the data of the order.

The method according to the present invention is of great advantage to the account manager as well; in fact, the account manager acts as an arbitrator of the transactions, since he is able to identify the identity of the participants in the transaction as well as the information transmitted by the same before the authorization is given to transfer any amount, thereby reducing the probability that fraud will be committed.
The codes used for at least partially encoding the data contained in the messages, together with the way said codes are communicated to the user as well as the double control of the data of the transaction, render the method according to the present invention suitable for execution commercial transactions with minimum risk yet with very high ease.

BRIEF DESCRIPTION OF THE DRAWINGS

Further advantages, objects and features as well as embodiments of the present invention as defined in the appended claims will become more apparent with the following detailed description when taken with reference to the accompanying drawings in which identical or corresponding parts are identified by the same reference numerals. In particular, in the drawings:

Fig. 1 represents in a schematic way a flow chart of a preferred embodiment of the method according to the present invention; moreover, in Fig. 1 there are depicted the essential parts of a preferred embodiment of the system according to the present invention adapted for executing the inventive method.

DETAILED DESCRIPTION OF THE INVENTION

While the present invention is described with reference to the embodiments as illustrated in the following detailed description as well as in Fig. 1, it should be understood that the following detailed description as well as Fig. 1 are not intended to limit the present invention to the particular illustrated embodiments disclosed, but rather the described illustrated embodiments merely exemplify various aspects of the present invention, the scope of which is defined by the appended claims.

With reference to Fig. 1, it is apparent that according to the preferred embodiment of the method and system of the present invention depicted therein, a user 1 is supplied in a usual way with at least a device 2 for gaining access to a communication network 3, such as, for instance, the internet. Said device 2 may comprise, for instance, a personal computer, a mobile phone GSM equipped with WAP or GPRS technology, a UMTS mobile phone, a web television or a similar device equipped with a software or hardware suit-
able for gaining access to the communication network 3 and/or for communicating through said communication network 3. By means of the access device 2, the user 1 may contact a merchant 4, for instance, by sending an e-mail message or by visiting one or more sites of a web site received in at least one processor 5, such as a web server or the like, connected to the communication network 3. In this way, the user 1 is able to select and order in a usual way one or more goods and/or services offered by the merchant 4. To this end, the processor 5 may comprise a database 6 containing a plurality of data records relating to the goods and/or services offered by the merchant 4. For instance, said data may comprise a description as well as a digital image along with the price of such goods and/or services. For the purpose of executing the order, the user 1 sends a message 7 to the merchant 4 through the communication network 3, with said message 7 containing at least a first code 8 identifying the user as well as other data, such as, for example, data 9 relating to the goods and/or services ordered and the prices of said goods and/or services. Additional data 10 may be contained in the message, such as, for example, the quantity and the delivery date of the goods and/or services ordered. The data 9 may correspond to one or more of the records contained in the data base 6 and the first code 8 identifying the user may, for instance, correspond to the number of the credit and/or debit cards of the user; alternatively, the first code 8 may correspond to the checksum number of the credit card of the user. The credit card may be one of the common credit cards, such as a Visa Card or MasterCard, or a credit card specially delivered to users who intend to execute commercial transactions according to the method of the present invention. Whichever card is used, said card may contain additional data of the user, for instance memorized in a magnetic band and/or a microchip. In addition, the first code 8 may be memorized in said magnetic band and/or microchip.

Submitting and/or sending the order by the user 1 to the merchant 4 may be executed in a usual way, for instance by using at least a page sent by the processor 5 and displayed on a screen 12 connected to the processing device 2. Said page may contain fields which can be filled in by the user 1 with the data requested as well as other useful information, such as, for example, a logo and/or mark certifying that the merchant 4 is allowed to execute the transaction according to the method of the present invention. Once the order 7 is received by the merchant 4, the merchant 4 may send to the user 1 a message 13, for instance an e-mail, by means of a processor, with said message 13 containing the confirmation of receipt of the order 7 along with a code 14 identifying the merchant 4 memorized in the processor. The message 13 may also contain a further code,
namely a code identifying the transaction (ID transaction), with said ID transaction having been previously assigned to the transaction by the merchant. Alternatively, the code 14 identifying the merchant may be previously communicated to the user, for instance by means of a posted letter. The processor used by the merchant for replying to the user by sending the message 13 may be the same processor 5 used for receiving the message 7 sent by the user 1. The message 13 may also contain a request that the order be confirmed by an account manager 15; also the account manager 15 may be equipped with a processor 16, for instance a web server connected to the communication network 3. For instance, the account manager 15 may be, a bank and/or an institute for managing credit and/or debit cards. According to a preferred embodiment, the account manager 15 previously assigns to the merchant 4 a code 14 identifying the merchant; in particular, said code 14 may be assigned to the merchant after a contract has been signed and the merchant 14 has been enabled and/or qualified to execute transactions according to the method of the present invention.

Still according to the present invention, the user 1, in order to confirm the order 7, sends a message 17 over the communication network 3 to a processor 16 of the account manager 15. For instance, said message 17 may be an e-mail containing a personal code 18 identifying the user 1 together with encoded data 19. Said personal code 18 may be a code previously furnished by the account manager 15 to the user 1; in particular, said personal code 18 may be submitted to the user with a posted letter or in person or in some other equivalent direct manner. Preferably, the personal code 18 is not furnished to the user 1 over the communication network 3. For instance, said personal code 18 may correspond to the pin number associated with the credit and/or debit card of the user 1 or even the number of the credit card of the user. The package of encoded data 19 may contain the code 14 identifying the merchant 4 and the data 9 and 10 relating to the order 7. Alternatively, the encoded data 19 may also contain the code identifying the transaction ID transaction), submitted by the merchant 4 to the user 1 with the message 13. Said data 19 are encoded by means of a program of a kind known in the art, with said program being executed by the device 2 according to a predefined coding key 21 inserted by the user 1 into the device 2. For instance, said encoding program may comprise an applet Java and may have been previously sent from the account manager 15 to the user 1 on a memory support such as a floppy disk; alternatively said encoding program may be transmitted in real time through the communication network 3. Preferably,
the encoding key 21 has not been submitted from the account manager 15 to the user 1 through the communication network 3, but by means of postal delivery or in person or even in some other direct manner. When the encoding key 21 is communicated by means of a message 22 on paper (for instance, a letter), said message is also provided with its own identifying code 23 and preferably contains a list of encoding keys 21 to be used only once. In order to be enabled to use the list of encoding keys 21, the user 1 has previously sent to the account 15, for instance through the communication network 3, confirmation of receipt comprising the personal code 18 and the code 23 identifying the list.

At the same time, the merchant 4 requests that the transactions be executed by sending a message 24 to the account manager over a processor connected to the communication network 3. For instance, said processor may be the same processor 5. The message 24 may be an e-mail containing the code 14 identifying the merchant, the first code 8 identifying the user, and the data 9, 10 relating to the order.

Once the messages 17 and 24 have been received by the merchant 15, a processor 16 of the account manager 15 selects a decoding key 27 from a table 25 contained in a database 26; said decoding key 27 is selected on the basis of the second code 18 identifying the user contained in the message 17. Pairs of the encoding and decoding keys 21 and 27, which have been assigned to each other and to the codes 23 identifying the lists 22, are also contained in the table 25; said encoding and decoding keys 21 and 27 are also assigned to the codes 18 identifying the users who have received said lists as well as to a variable 28 indicating that the keys 21 and 27 have been used. The variable 28 changes its value each time a pair of the keys 21 and 27 is used. Once the keys 21 and 27 have been used, the decoding keys 27 and the corresponding records in the table 25 may be cancelled. The decoding key 27 used for decoding the data of a predefined message is the first key of those assigned to the user 1 who sends the message 17; which have not yet been used. Said decoding key 27 is used by the processor 16 together with the decoding program to obtain the data contained in the package 19 of encoded data, namely the code 14 identifying the merchant and the data 9 and 10 relating to the order.
Furthermore, the processor 16 extracts or generates from a table 29 a further code identifying the user 1 on the basis of to the personal code 18 contained in the message 17. As it will be apparent in the following, said further code identifying the user normally corresponds to the first code 8 identifying the user. If the further code generated corresponds to the first code 8 and other conditions are met the transaction can be executed. If the further code generated does not correspond to the first code or other conditions are not met the transaction is stopped. The table 29 may be contained in the database 26 and contains the pairs of codes 18 submitted to the users 1 and the further codes to be generated (normally corresponding the first codes 8), as well as other data such as, for example, the name and the address of the users. The processor 16 comprises a table 31 contained in the database 26, with said table 31 containing, in turn, the codes 14 identifying the merchants 4 enabled to execute transactions according to the method of the present invention.

Once the further code (normally corresponding to the code 8) contained in the table 29 as well as the code 14 identifying the merchant 4 and the data 9 and 10 contained in the message 17 have been obtained, the processor 16 checks whether the code 14 identifying the merchant 4 is contained or not in the table 31; if the code 14 is contained in the table 31, the processor 16 checks whether a message has been received, for instance a message 24, and whether the code 14 contained in said message 24 corresponds to the code 14 contained in the table 31. If such a message has not been received, the processor 16 stands in standby waiting to receive such a message; on the other hand, namely if such a message has been received, the processor 16 checks whether other data contained in the messages 17 and 24 received from the user 1 and the merchant 4 correspond; in particular, the processor 16 checks whether the decoded data 9 and 10 extracted from the message 17 and relating to the order correspond to the data 9 and 10 contained in the message 24. Moreover, the processor 16 checks whether the further code as extracted from the table 29 corresponds to the code 8 identifying the user 1 as contained in the message 24. If the data corresponds the processor 16 confirms and/or executes the transaction, for instance charging the user 1 an amount corresponding to that indicated in the data 9 relating to the order; in the same way, a corresponding amount is transferred to the merchant 4, eventually minus a provision for the service rendered.
If the message 24 is not received within a predefined time limit, for instance within the delivery date indicated in the data 10 relating to the order, and if further conditions necessary for the execution of the transaction are not met, the transaction is not executed. For instance, if comparing the data contained in the messages 17 and 24 reveals that the data do not correspond the transaction is stopped. Other conditions may comprise a confirmation message either from the user 1 or the merchant 4; the transaction is also not executed in the case that the message 24 is received but said message 24 does not correspond to the message 17.

The fact that the transaction has not been executed or has not been executed properly may be communicated from the account manager 15 to the user 1 and/or to the merchant 4 by sending corresponding messages 32, 33 by means of the processor 16; for instance, said messages may contain e-mails sent over the communication network 3.

Of course, it should be understood that a wide range of changes and modifications can be made to the embodiments described above without departing from the scope of the invention. For instance, it appears clearly to those skilled in the art that the system according to the present invention for executing commercial transactions may comprise a plurality of users 1 as well as a plurality of merchants 4 and account managers 15; each of said subjects may, in turn, be provided with a plurality of devices and/or processors for obtaining access to the communication network 3 as well for executing one or more steps of the method according to the present invention.

It is therefore understood that it is the claims, including all equivalents, which are intended to define the scope of the invention. It is also to be noted that the forms of the present invention described therein represent the presently preferred embodiments.
Claims

1) A method of transmitting data over a communication network (3) to which comprising at least three computer systems (2, 5, 16) are connected, said method comprising:

sending a first message (7) from a first one (2) of said at least three computer systems to a second one (5) of said at least three computer systems (5), with said first message (7) containing at least a first code (8) and data (9, 10);

sending a second message (24) from the second computer system (5) to at least a third one (16) of the at least three computer systems, with said second message (24) containing a second code (14) as well as the first code (8) and the data (9, 10);

sending a third message (17) from the first computer system (2) to the third computer system (16), with said third message (17) containing a third code (18) as well as encoded data (19) containing the second code (14) and the data (9, 10);

wherein the third computer system (16) performs the steps of:

decoding the encoded data (19) to extract the second code (14) and the data (9, 10) from the encoded data (19);

generating a fourth code on the basis of the code (18);

comparing the extracted data (9, 10) with the data (9, 10) contained in the second message (24);

comparing the extracted code (14) with the second code (14) contained in the second message (24);

comparing the fourth code with the first code (8) contained in the second message (24).
2) A method as claimed in claim 1, wherein further messages (32, 33) are sent by the third computer system (16) to the first and second computer systems (2, 5) depending on the result of the at least one comparison steps.

3) A method as claimed in one of claims 1-2, wherein the first computer system (2) is used by a user (1), the second computer system (5) is used by a merchant (4) and the third computer system (16) is used by an account manager (15) for executing commercial transactions.

4) A method as claimed in claim 3, wherein an amount is charged on the user (1) by the third computer system (16) of the account manager (15) depending on the result of at least one comparison steps.

5) A method as claimed in one of claims 1-4, wherein the second computer system (5), after receipt of the first message (7), sends a fourth message (13) to the first computer system (2) containing a confirmation of receipt of the first message (7) as well as the second code (14).

6) A method as claimed in one of claims 3-5, wherein the first code (8) and the third code (18) identify the user (1), and the second code (14) identifies the merchant (4).

7) A method as claimed in one of claims 3 to 6, wherein the transaction is stopped if the fourth code does not correspond to the first code (8) contained in the second message (24).

8) A method as claimed in one of claims 3-7, wherein the transaction is stopped if the extracted data (9, 10) do not correspond to the data (9, 10) contained in the second message (24).

9) A method as claimed in one of claims 3-8, wherein the transaction is stopped if the extracted code (14) does not correspond to the code (14) contained in the second message (24).
10) A method as claimed in one of claims 1 to 9, wherein the encoded data (19) contained in the third message (17) are encoded by means of a program executed by the computer system (2) according to an encoding key (21).

11) A method as claimed in one of claims 1-10, wherein the encoded data (19) contained in the third message (17) are decoded by means of a computer program executed by the computer system (16) according to a decoding key (27).

12) A method as claimed in claim 11, wherein the decoding key (27) is assigned to the third code (18) and contained, together with said third code (18), in a data base (26) connected to the third computer system (16).

13) A method as claimed in claim 12, wherein the decoding key (27) is disabled or cancelled after use.

14) A system for transmitting data over a computer network (3), said system comprising at least a first computer system (2), a second computer system (5) and a third computer system (16) adapted to be connected to the communication network (3), wherein

said at least first computer system (2) is adapted to send at least a first message (7) to at least the second computer system (5), with said first message (7) containing at least a first code (8) and data (9, 10);

said at least second computer system (5) is adapted to send at least a second message (24) to the third computer system (16), with said second message (24) containing a second code (14) as well as the first code (8) and the data (9, 10);

said at least first computer system (2) is adapted to send at least a third message (17) to the at least third computer system (16), with said third message (17) containing a third code (18) as well as encoded data (19) containing the second code (14) and the data (9, 10);

with said at least third computer system (16) comprising means for performing the following steps:
decoding the encoded data (19) to extract the second code (14) and the data (9, 10) from the encoded data (19);

generating a fourth code on the basis of the third code (18);

comparing the extracted data (9, 10) with the data (9, 10) contained in the second message (24);

comparing the extracted code (14) with the second code (14) contained in the second message (24);

comparing the fourth code with the first code (8) contained in the second message (24).

15) A system as claimed in claim 14, wherein the third computer system (16) is adapted to send further messages (32, 33) to the first and second computer systems (2, 5) depending on the result of at least one of the comparison steps.

16) A system as claimed in one of claims 14-15, wherein said first, second and third computer system (2), (5) (16) are adapted to be used by a user (1), a merchant (4) and an account manager (15), respectively, for executing commercial transactions.

17) A system as claimed in claim 16, wherein the third computer system (16) is adapted to charge an amount on the user (1) depending on the result of at least one of the comparison steps.

18) A system as claimed in one of claims 14-17, wherein the second computer system (5) is adapted to send a fourth message (13) to the first computer system (2) after receipt of the first message (7), with said fourth message (13) containing a confirmation of receipt of the first message (7) as well as the second code (14).

19) A system as claimed in claim 16-18, wherein the third computer system (16) further comprises means for stopping the transaction if the fourth code generated does not correspond to the first code (8) contained in the second message (24).
20)  A method as claimed in one of claims 16-19, wherein the third computer system (16) further comprises means for stopping the transaction if the extracted data (9, 10) do not correspond to the data (9, 10) contained in the second message (24).

21)  A method as claimed in one of claims 16-20, wherein the third computer system (16) further comprises means for stopping the transaction if the extracted code (14) does not correspond to the second code (14) contained in the second message (24).

22)  A system as claimed in one of claims 14-21, wherein the first computer system (2) is adapted to execute a program for encoding the data (19) contained in the third message (17) according to an encoding key (21).

23)  A system as claimed in one of claims 14-22, wherein the third computer system (16) is adapted to execute a program for decoding the encoded data (19) contained in the third message (17) according to a decoding key (27).

24)  A system as claimed in claim 23, wherein the third computer system (16) is connected to a data base (26) containing the decoding key (27) and the code (18).

25)  A system for transmitting data over a computer network (3), said system comprising at least a first computer system (2) and a second computer system (16) adapted to be connected to the communication network (3), wherein

said at least first computer system (2) is adapted to send at least a first message (17) to the at least second computer system (16), with said first message (17) containing a first code (18) as well as encoded data (19) containing a second code (14) and data (9, 10); with said at least second computer system (16) comprising means for performing the following steps:

decoding the encoded data (19) contained in the first message (17) to extract the second code (14) and the data (9, 10) from the encoded data (19);
generating a third code (8) on the basis of the first code (18);

comparing the extracted data (9, 10) with corresponding data (9, 10) contained in a second message (24);

comparing the extracted code (14) with a corresponding code (14) contained in the second message (24);

comparing the third code (8) with a corresponding code (8) contained in the third message (24).

26) A system as claimed in claim 25, wherein the second computer system (16) is adapted to send further messages (32, 33) to the first computer system (2) depending on the result of at least one of the comparison steps.

27) A system as claimed in one of claims 25-26, wherein said first and second computer system (2), (16) are adapted to be used by a user (1) and an account manager (15), respectively, for executing commercial transactions.

28) A system as claimed in claim 27, wherein the second computer system (16) is adapted to charge an amount on the user (1) depending on the result of at least one of the comparison steps.

29) A system as claimed in claim 27-28, wherein the second computer system (16) further comprises means for stopping the transaction if the third code generated does not correspond to the code (8) contained in the second message (24).

30) A system as claimed in one of claims 27-29, wherein the second computer system (16) further comprises means for stopping the transaction if the data (9, 10) extracted from the first message (17) do not correspond to the data (9, 10) contained in the second message (24).

31) A system as claimed in one of claims 27-30, wherein the computer system (16) further comprises means for stopping the transaction if the code extracted from the first
message (17) does not correspond to the code (14) contained in the second message (24).

32) A system as claimed in one of claims 25-31, wherein the first computer system (2) is adapted to execute a program for encoding the data (19) according to an encoding key (21).

33) A system as claimed in one of claims 25-32, wherein the second computer system (16) is adapted to execute a program for decoding the encoded data (19) according to a decoding key (27).

34) A system as claimed in claim 23, wherein the second computer system (16) is connected to a data base (26) containing the decoding key (27) and the third code (18).