OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

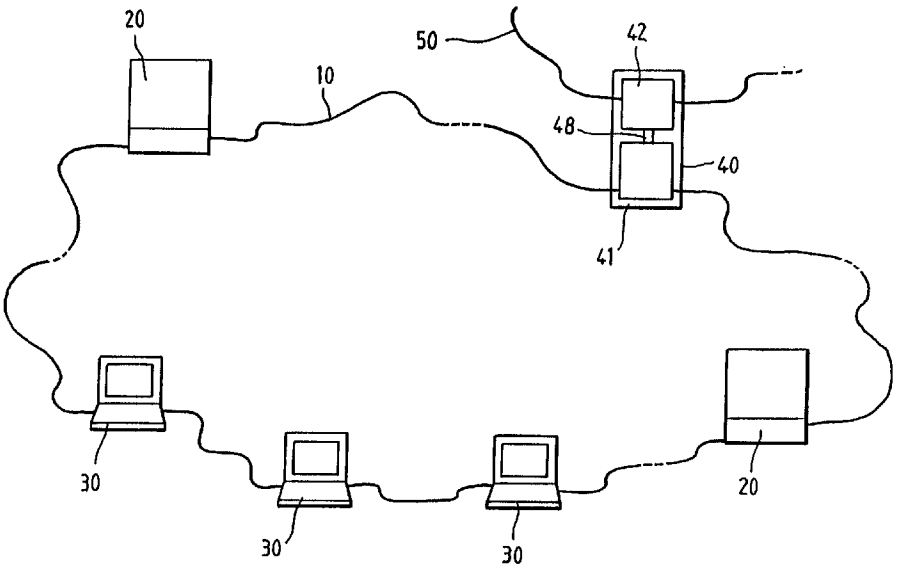
(21) (A1) **2,217,739**
(86) 1996/04/03
(87) 1996/10/17

(72) PAYS, Paul-André, FR
(72) DAHAN, Gérard Ben, FR
(71) G C TECH, FR

(51) Int.Cl.[6] G07F 7/00
(30) 1995/04/14 (95/04533) FR

(54) **PROCEDE DE PAIEMENT ELECTRONIQUE PERMETTANT D'EFFECTUER DES TRANSACTIONS LIEES A L'ACHAT DE BIENS SUR UN RESEAU INFORMATIQUE**

(54) **ELECTRONIC PAYMENT METHOD FOR PURCHASE-RELATED TRANSACTIONS OVER A COMPUTER NETWORK**



(57) Le procédé utilise un réseau de communication ouvert (10) sur lequel sont connectés des postes serveurs de marchands (20) et des postes clients (30) et comprend: l'élaboration par un poste serveur de marchand d'un ticket de paiement, concernant un achat envisagé entre le marchand et un client, et comportant des informations relatives au marchand, au client, à l'objet de l'achat et à son prix; la transmission du ticket de paiement via le réseau à un poste serveur de paiement (40); la vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, soit par interrogation d'un compte client propre au client,

(57) A method using an open communication network (10) to which retailer server stations (20) and customer stations (30) are connected. According to the method, a retailer server station generates a payment slip for the planned purchase transaction between the retailer and a customer, which slip comprises data on the retailer, the customer, the purchased item or service and the price; the payment slip is transmitted over the network to a payment server station (40); the payment server automatically checks whether the payment of said price is authorised for the customer in question, by querying the client's personal account set up in the payment server

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(21) (A1) **2,217,739**
(86) 1996/04/03
(87) 1996/10/17

tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par interrogation sur un réseau bancaire (50) indépendant du réseau informatique (10), pour les paiements de montants plus élevés; si la vérification est positive, l'élaboration par le serveur de paiement d'un bon de caisse comportant au moins une partie des informations du ticket de paiement; et la transmission du bon de caisse au serveur de marchand afin d'autoriser la réalisation de l'achat.

for paying small amounts, or, in the case of larger amounts, by making a query over a banking network (50) separate from the computer network (10); if the payment is authorised, the payment server generates a cash voucher comprising at least some of the data on the payment slip; and the cash voucher is transmitted to the retailer to enable the purchase to go ahead.

ABSTRACT

The method uses a public communication network (10), to which are connected supplier servers (20) and customer stations (30) and comprises:

– development by a supplier server of a payment ticket, concerning a purchase envisaged between the supplier and a customer, and comprising information relating to the supplier, the customer, the purchase object and the price,

– transmission of the payment ticket via the computer network to a payment server (40),

– automatic verification by the payment server if the payment of the price is authorised for the customer, either by interrogation of a customer account of the customer, held by the payment server and intended for payment of small sums, or by interrogation on a banking network (50) independent of the computer network (10), for payment of higher sums,

– if the verification is positive, development by the payment server of a voucher including at least a part of the payment ticket information, and

– transmission of the voucher to the supplier server so as to authorise the conclusion of the purchase.

Figure 1.

ELECTRONIC PAYMENT METHOD FOR PURCHASE-RELATED TRANSACTIONS OVER A COMPUTER NETWORK

The present invention concerns an electronic payment method enabling transactions to be carried out relating to the purchase of "goods" offered by suppliers by means of on-line services via a public computer telecommunication network to which are attached suppliers' servers and clients' stations. Here, "public computer telecommunication network" is intended to mean a network to which persons or companies can freely connect themselves so long as they have an address, for example the "Internet". "Goods" is intended to mean products or services, which are delivered outside the network after the transaction has been concluded, as well as non-material goods, such as information, which can be delivered via the computer network.

Various electronic payment methods have been proposed, and some are already operational.

Several methods are based on a new form of currency. They involve an electronic representation, sometimes called a "token", which can be purely embodied in software or can be partly physical, for example a "smart card". These methods necessitate circulation of the currency on the computer network, which presents difficult security problems regarding the creation of false currency.

Other known electronic payment methods necessitate a direct relation with a bank or a banking network. These are typified by methods used in the credit card networks such as well-known methods utilizing point-of-sale terminals linked to a bank card circuit as well as methods employing electronic cheques using an electronic signature to authenticate the purchaser. This is a form of engagement letter issued by a purchaser, returned to the seller and accepted and recognised by a bank.

There are certain inconveniences associated with methods which necessitate, at one time or another during a transaction, a relationship with a traditional banking system and the effecting of a transaction in such a system. Banking system transactions have a real cost which becomes prohibitive when the amount of the purchase is very low, for example, an amount based on a query to a data base. And computer networks are well adapted to the sale of low-priced goods, in particular informational goods, since the delivery can be carried out through the network itself. Moreover, access to a banking network or a bank card network must have high levels of security, which, in practical terms, excludes the

possibility of access through a public computer network, such as the "Internet", to which potential purchasers can connect themselves.

An object of the invention is to provide a method which avoids the problems of the known methods – in particular, a method permitting a simple and reliable way of accomplishing transactions relating to the purchase of goods on a computer network, without the need to circulate electronic currency, for goods of high price requiring authorisation from a traditional banking system, as well as for goods of low to very–low price.

The object is achieved by a method of the type defined at the beginning of the present description and comprising, according to the invention, the steps of:

–creation, by the server of a supplier connected to the network, of a transaction authorisation request or "payment ticket", concerning a purchase envisaged between the supplier and a customer, and comprising information relating to the supplier, the customer, the purchased object and the price;

–transmission of the payment ticket via the computer network to a payment server which is distinct from the customer station and the supplier server,

–automatic verification by the payment server of whether the payment of the price is authorised for the customer involved, the verification being effected, according to the level of the price to be paid, either by interrogation of an account of the customer, held by the payment server and intended for payment of smaller sums, or by interrogation on a banking network, independent of the computer network, for payment of higher sums;

–if the verification is positive, creation by the payment server of a transaction authorisation or voucher including at least part of the payment ticket information; and

–transmission of the voucher to the supplier server via the computer network, to authorise the conclusion of the purchase.

Thus, the procedure according to the invention is noteworthy in that it necessitates neither the creation of electronic currency nor the circulation of electronic currency over the computer network.

The control of the transactions is effected by a payment server which alone can access a banking network or a bank card network, and which manages non–bank customer accounts from which small sum transactions can be effected.

The payment server also manages non–bank supplier accounts used for small sum transactions. In this way, when a voucher is transmitted after verification by interrogation of a customer account held by the payment server, the

amount of the purchase is debited from the customer account and credited to the account of the concerned supplier and held by the payment server, a procedure which does not produce high processing costs.

Each customer has available his own identity to enable use of the payment method. He must also have available a real bank account, preferably one which can be operated by means of traditional bank cards. The verification by the payment server can include a preliminary phase of validating the identity of the customer from the contents of the payment ticket. The identity validation precedes access to the customer account (if the sum of the purchase is low) or access to the bank network (if the amount involved in the purchase is higher). The payment server preferably includes means, for example a data base, for storing the relationship between the customer identities used for transactions on the computer network and the bank identities (bank account or credit card numbers) used for transactions on the bank network. In that way, the circulation of banking identities on the computer network can be avoided.

An implementation of the invention will now be described, as a non-limiting example, with reference to the accompanying drawings, in which:

–Figure 1 is a general schematic view of an electronic payment system according to the invention;

–Figure 2 is a representation in the form of a block schematic diagram of a payment server of the system of Figure 1;

–Figure 3 illustrates the progression of operations relating to a purchase using the system of Figure 1; and

Figures 4A to 4C are flow charts showing schematically the operations carried out by the payment server.

Figure 1 represents schematically a computer telecommunication network 10 to which are connected supplier servers 20, customer stations 30 and at least one payment server 40.

The computer network 10 is an open or public network, for example the network known as the "Internet". The supplier servers 20 are units such as those currently used for on-line services connected to the Internet, for example, units organised around UNIX-based multi-processor machines. The customer stations 30 are basically microcomputers which are provided with means for connecting to the Internet network 10, for example, in the form of a "Web" interface. The supplier servers 20 and the customer stations 30 may use, for example, known

software protocols commonly known as the "World Wide Web" ("WWW") employing the HTTP protocol.

The payment server 40, shown in more detail in Figure 2, comprises front and rear units respectively 41 and 42 both connected to the Internet 10. The front unit 41 has an architecture similar to that of a standard server connected to a network such as the Internet. The rear unit 42 includes a processing unit 43 containing one or more processors, a data base 44 containing information relating to the suppliers and customers subscribing to the payment system, a transaction register 45, an interface unit 46 for connecting with a banking network or with a bank card network 50, and a communication bus 47 or similar other link enabling connection between the different constituent parts of the unit. A secure connection 48 enables bi-directional communication between the front unit 41 and the processing unit 43. Communication with the network 10 is controlled by the front unit 41 while management of the data base 44 as well as the control of the communication with the banking network are assured by the rear unit 42.

The data base 44 contains information relating to the customers and to the suppliers who have subscribed to the payment system. For each customer, the data base 44 contains the system identity ("**CId**") assigned when the customer initially subscribes to the system, a customer account or electronic wallet ("**PME**") for payment of small sums, a banking identity such as an account number of a real account or a credit card number, possibly as well as the customer's own access password or "key". For each supplier, the data base 44 contains the system identity of the supplier/merchant ("MId"), which is assigned when the supplier initially subscribes to the system, a supplier account, or electronic cash register ("**TCE**") for receipt of small sums and a banking identity such as a bank account number.

Figure 3 shows schematically the different stages of a transaction relating to the purchase of goods by a subscribing customer from a subscribing supplier. It can be a case of material goods, for which delivery to the customer will take place after conclusion of the transaction, or non-material goods (such as information) which can be provided to the customer over the computer network as soon as electronic payment has been effected.

(1) Consultation by the customer

After connecting to the Internet 10, a customer can consult the catalogue or "window" of any supplier on-line by accessing the supplier's server 20 and viewing the supplier's wares on the screen of the customer station 30. On presentation of the customer's system identity **CId**, the supplier's server 20 can

present to the customer particular financial conditions (for example a discount) applicable to the potential transaction.

(2) Purchase demand

Once the customer has chosen a commodity (object) O, his choice is transmitted to the supplier's server in the form of a message containing an identity **OId** of the commodity and the identity **CId** of the customer. When necessary, for example, for the eventual delivery of the commodity chosen, the supplier's server can request supplementary information such as an address and preferred delivery time. This may conveniently be done through use of an electronic form sent over the network to be filled in by the customer.

When the purchase envisaged represents a large sum or is subjected to legal conditions, a preliminary authentication of the customer may be desired. As will be seen in detail in the following, the authentication of a customer is effected by the payment server 40. Also, the authentication demand coming from a supplier is advantageously issued in the form of a payment ticket of no value which is transmitted to the payment server over the computer network via the customer station and, in the case of positive authentication, provokes the return of a voucher from the payment server to the supplier server, always by way of the customer station. The procedure for the establishment of a payment ticket and for the returning of a voucher are described in greater detail in the following.

The purchase demand issued by the customer can relate to a single commodity or to several goods to be provided as a group "basket purchase".

(3) Development of the payment demand

In response to a purchase demand, the supplier server develops a payment demand, which can include the following information:

- Identity of the supplier ("**MId**");
- Description of the commodity ordered, or, in the case of grouped purchases, each of the goods in the basket;
- Type of transaction (single or basket);
- Identity of the customer ("**CId**");
- Identity of the commodity or collection of goods of the basket ("**OId**");
- Price of the commodity ("**Oid**");
- Value Added Tax, VAT, (if applicable),
- Date and time of the issue of the payment ticket (hour and date stamping by the supplier server);
- Period of validity of the payment ticket; and

–Serial number in the sales register of the supplier (particularly in the case when the transaction has included a preliminary authentication stage).

The combination of the above information is coded as a series of bytes which are contained in the hidden channel of a payment ticket (or URL of an order of a commodity, URL being the initials of "Uniform Resource Locator" used in WWW software with the HTTP protocol), as follows:

URL http:<SP><description of the order>,

where SP is the Internet address of the payment server. The payment ticket is addressed to the customer station. It is completed by two logical "anchors" which enable the customer either to cancel or to confirm.

(4) Sending the payment order

The payment order is transmitted to the payment server simply by validation by the customer of the URL of the payment order. As will be appreciated, the payment ticket only passes in transit through the customer station.

(5) Issue of the voucher

Upon reception of a payment order, the payment server 40 decodes the payment order, authenticates the customer and investigates whether the payment can be authorised before returning either a voucher or a payment refusal. The customer authentication and payment authorisation operations will be described in greater detail with reference to Figure 4.

When the verification process does not permit authorisation of payment, an explanatory refusal notification (referring, for example, to insufficient funds in the account, to the passing of a limit authorised for the customer, etc.) is sent to the customer by the payment server. When the verification does permit authorisation of payment, the information contained in the payment ticket is completed with a serial number in the transaction register 45, a time stamp, a validity time limit (typically some tens of seconds) and the seal of the payment server constituting certification information. The combination of this information, possibly after being digitally signed through use of a private key portion of a public key/private key encryption system belonging to the payment server (which ensures the validity and the integrity of the payment authorisation) is encoded in a series of bytes which constitute the hidden channel of a voucher or delivery URL:

URL http:<M><description of the voucher>,

where M is the Internet address of the supplier.

(6) Delivery request

The voucher is transmitted to the supplier server via the customer station. This can be effected automatically by the software installed in the customer station using the re-routing possibility of the URLs, well-known to those skilled in the art to which the invention pertains. The supplier server decodes and verifies the received voucher before authorising delivery of the commodity. This verification includes using the private key of the payment server, verifying that the validity time limit has not passed and comparing the contents of the voucher with the payment demand.

(7) Delivery of the commodity

When the voucher has been validated by the supplier server, this server can effect delivery directly to the customer station, in the case where the commodity being purchased is information, or address to the customer station a document permitting the collection of the commodity and, notably, specifying the place of delivery and the name of the recipient.

It will be noted that, in the case of a grouped or basket purchase, the supplier server creates an object with allocation of a unique identity, a list of the URLs of each of the goods contained in the basket. It is this object which is indicated in the URL commodity order and which enables the details of the purchased goods to be recorded in the transaction register of the payment server.

Figures 4A to 4C show the operations carried out by the payment server 40 in response to the reception of a payment order.

In the front unit 41(Figure 4A), the payment order is decoded (stage 61) and its validity is examined (test 62) notably from the point of view of the validity period. If the result of the examination is negative, a refusal notification is sent to the customer station (stage 63). If the result of the examination is positive, customer authentication follows (stage 64). The details of this operation are described further with reference to Figure 4C. If the authentication is negative (test 65), a refusal notification is sent to the customer (stage 63). If the authentication produces a positive result, the payment order (possibly limited to the customer identity **CId**, the supplier identity **MId** and the price) is transmitted via the communication stage 68 to the rear unit 42 of the payment server shown in Figure 2 (stage 66). The connection 48, as mentioned above, is a secure connection preventing access to the rear unit by persons connected to the network 10.

The front unit 41 then waits for the rear unit to determine whether or not to authorise the payment (stage 67). If the payment is not authorised, (test 68), a refusal notification is sent to the customer station (stage 63). If the payment is

authorised, a voucher is prepared (stage 69) using the information recorded in stage 62. The voucher is saved in a memory of the front unit 41 (stage 70) and is sent to the supplier server via the customer station (stage 71).

In the rear unit 42 (Figure 4B) of the payment server, a newly received and authenticated payment order is examined to determine whether this order should be authorised from the customer account **PME** or through the banking network. In this respect, the price is compared with a minimum threshold (test 72). This threshold is, for example, some tens of French francs.

If the threshold is exceeded, a request for effecting the payment operation is sent to the banking network (stage 73) using the banking identity corresponding to the customer identity **CId** as obtained from consultation of the data base 44. The positive or negative response from the banking network (stage 74), when received, is transmitted to the front unit 41 (stage 75).

If the threshold is not exceeded, the payment can be effected from the **PME** customer account.

In this event, the customer account is examined to determine whether it has sufficient funds (test 76). If it does not, a refusal of payment authorisation is sent from the rear to the front unit (stage 75). If it does, the price is debited from the **PME** customer account, the **TCE** supplier account corresponding to the identity **MId** is credited with the same sum (stage 77), the transaction is inscribed in the transaction register 45 (stage 78), and the payment authorisation – in other words, a positive response – is transmitted to the front unit 41 with the indication of the serial number of the inscription in the transaction register (stage 75).

The authentication procedure in the payment server (Figure 4C), at the stage 64 of Figure 4A, comprises sending to the customer station, preferably in secure (encrypted) form, a demand for an access key, or password (stage 641). Upon reception, in secure form, of the access key (stage 64), a comparison is effected between corresponding information contained in the data base 44 (test 643). If the comparison is negative, and a maximum number of unsuccessful attempts has not been reached (test 644), the process returns to stage 641. If this maximum number has been reached, the failure to authorise is noted, and an alert is produced (stage 645) and a negative response is sent to the customer station (stage 646). The alert can comprise cancellation of the **PME** account or surveillance of this account in order to detect new usage attempts. If the test at step 643 is positive, the authentication is recorded (stage 647) and a positive response is provided (stage 648).

Different encoding techniques for permitting secure transmission of numeric information in a computer network are well known, notably for the request and sending of access keys.

The authentication procedure disclosed herein permits a preliminary authentication of a customer to be effected when necessary before the establishment of a payment demand by the supplier's server. For this authentication, it is sufficient to create a payment ticket in which the price indicated is zero, as indicated above.

The recording of the voucher in the front unit permits the customers and the suppliers to carry out controls and, possibly, to obtain copies of these. The recording of transactions in the rear unit enables records of the transactions to be conserved for possible use when needed later, for example, in the case of a dispute arising between a customer and a supplier.

The balance in the customer accounts **PME** managed by the payment server is limited in size and, according to the preferred embodiment of the invention, these accounts do not receive interest payments (the payment system being separate from the banking world). Replenishment by a customer of his **PME** account can be effected from his bank account, by placing an order with his banking establishment.

The supplier accounts **TCE** managed by the payment server are associated with real bank accounts of the suppliers, into which they are, for example, emptied daily.

Although there has been described above one way of putting into effect the method according to the invention in an Internet environment and with WWW software using the HTTP protocol, a person skilled in the art will readily appreciate that the method can be put into effect with a network other than Internet or further with supplier servers and customer station software which does not use the HTTP protocol of WWW. Furthermore, secure authentication methods using apparatus such as smart card readers or voiceprint recognition means can be foreseen in the place of access keys. These and other variations which will occur to those skilled in the art are within the spirit and scope of the present invention.

CLAIMS

1. A method for effecting electronic payments for transactions relating to the purchase of goods offered by suppliers to customers via a public computer network, to which are connected supplier servers and customer stations, characterised by the steps of:

(a) development, by a supplier server connected to the network, of a transaction authorisation request, or payment ticket, concerning a purchase envisaged between the supplier and a customer, and comprising information relating to the supplier, the customer, the purchase object and the price,

(b) transmission of the payment ticket via the computer network to a payment server which is distinct from the customer station and supplier server,

(c) automatic verification by the payment server if the payment of the price is authorised for the customer, the verification being effected, according to the level of the price to be paid, either by interrogation of a customer account of the customer, held by the payment server and intended for payment of small sums, or by interrogation of a banking network, independent of the computer network, for payment of higher sums,

(d) if the verification is positive, development by the payment server of a transaction authorisation or voucher including at least a part of the payment ticket information, and

(e) transmission of the voucher to the supplier server via the computer network, so as to authorise the conclusion of the purchase.

2. A method as claimed in claim 1, characterised in that when a voucher is transmitted after verification by interrogation of a customer account held by the payment server, the amount of the purchase is debited from the customer account and credited to the supplier account of the concerned supplier and held by the payment server.

3. A method as claimed in claim 1 or 2, characterised in that the verification by the payment server comprises a preliminary customer authentication phase.

4. A method as claimed in claim 3, characterised in that the authentication is achieved by recognition of an access key transmitted by the computer network from the customer station to the payment server.

5. A method as claimed in any one of claims 1 to 4, characterised in that it comprises the development by the payment server of a voucher comprising at least a part of the information of the payment ticket and certification information.

6. A method as claimed in any one of claims 1 to 5, characterised in that it comprises memorisation by the payment server of the authorised transactions, by stocking at least a part of the contents of the voucher.

7. A method as claimed in any one of claims 1 to 6, characterised in that the payment ticket is transmitted from the payment server to the supplier server by the intermediary of the customer station.

8. A method as claimed in any one of claims 1 to 7 characterised in that the voucher is transmitted from the payment server to the supplier server by the intermediary of the customer station.

9. Electronic payment system for effecting transactions relating to the purchase of goods offered by suppliers to customers via a public computer network, the system comprising customer stations and supplier servers,

characterised in that the system further comprises at least one payment server distinct from the customer stations and the supplier servers and comprising:

–a front unit having means for connecting to the public network,

–a rear unit having means for connecting to a banking network independent of the public network,

–means for communicating between the front and rear units,

–means for memorising customer accounts and supplier accounts, and

–processing means for verifying, in response to the reception by the front unit of a transaction authorisation request or a payment ticket, concerning a purchase envisaged between the supplier and a customer, if the payment of the price is authorised for the customer by interrogating the customer account or the banking network, and, if the verification is positive, developing a transaction authorisation, or voucher in order to transmit the verification to the open network via the front unit.

10. Payment system as claimed in claim 9, characterised in that the payment server comprises means for memorising authorised transactions.

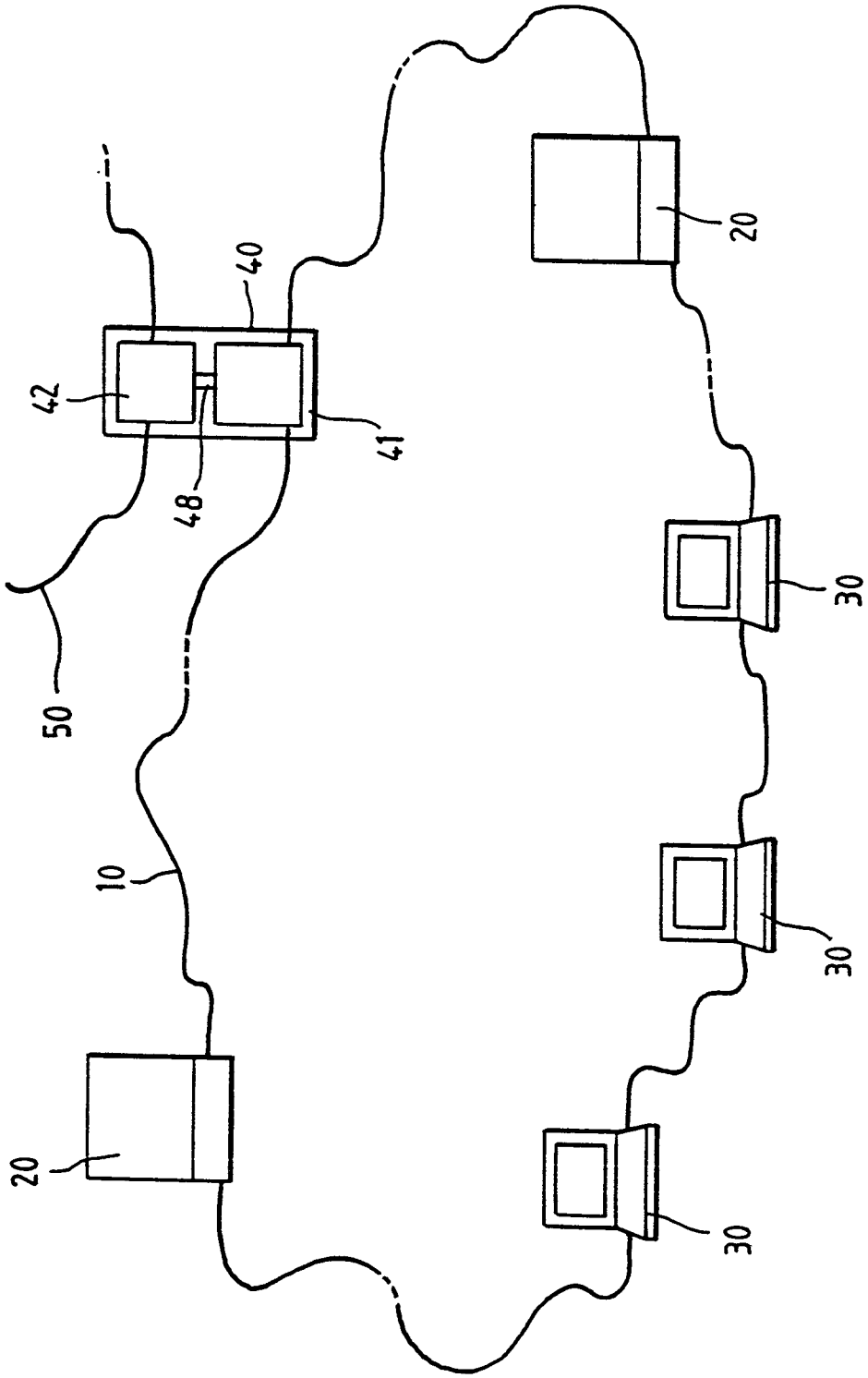


FIG.1

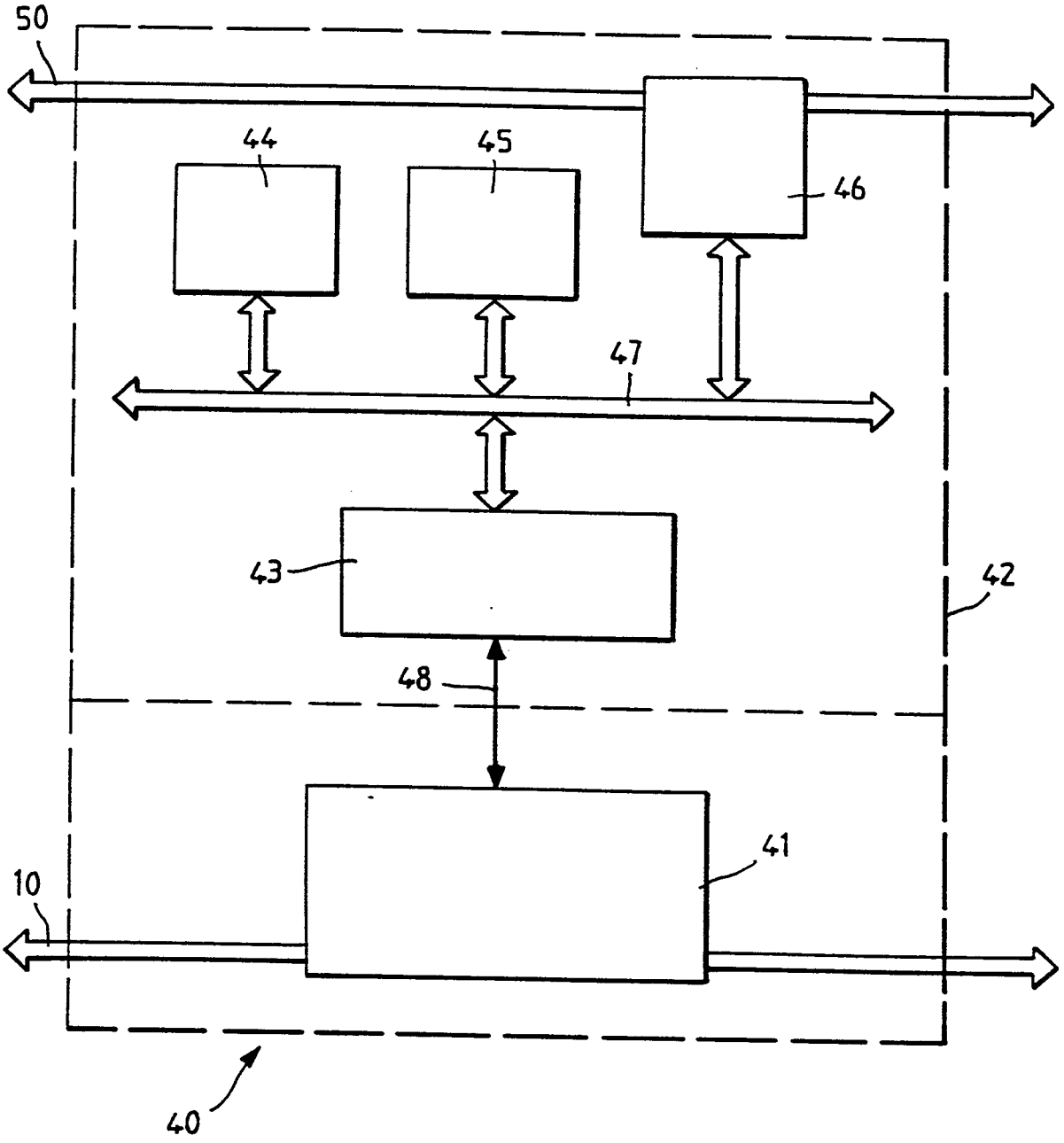


FIG. 2

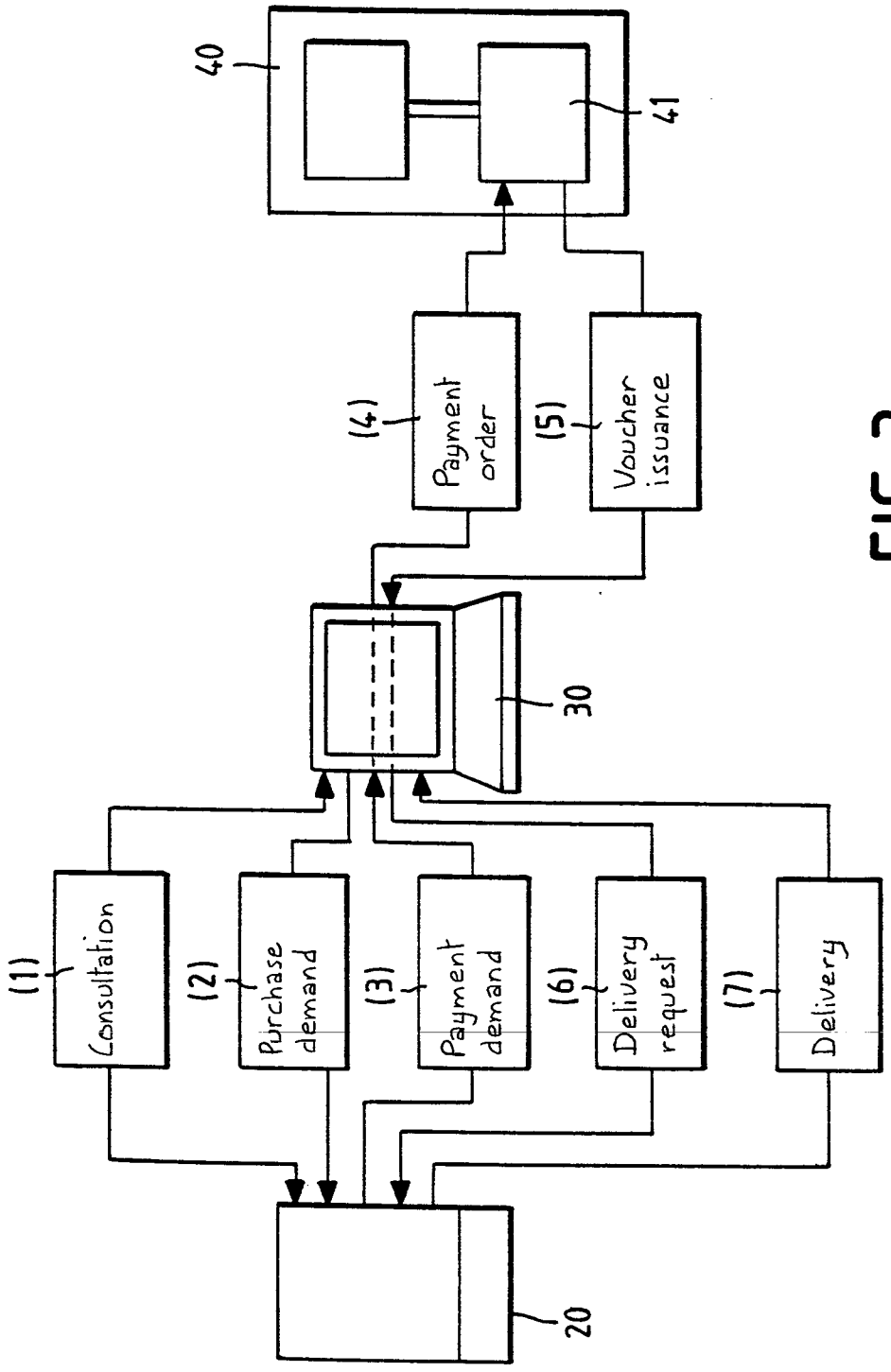

40
41
(4)
Payment order
(5)
Voucher issuance
30
(1)
Consultation
(2)
Purchase demand
(3)
Payment demand
(6)
Delivery request
(7)
Delivery
20

FIG. 3

FIG. 4A

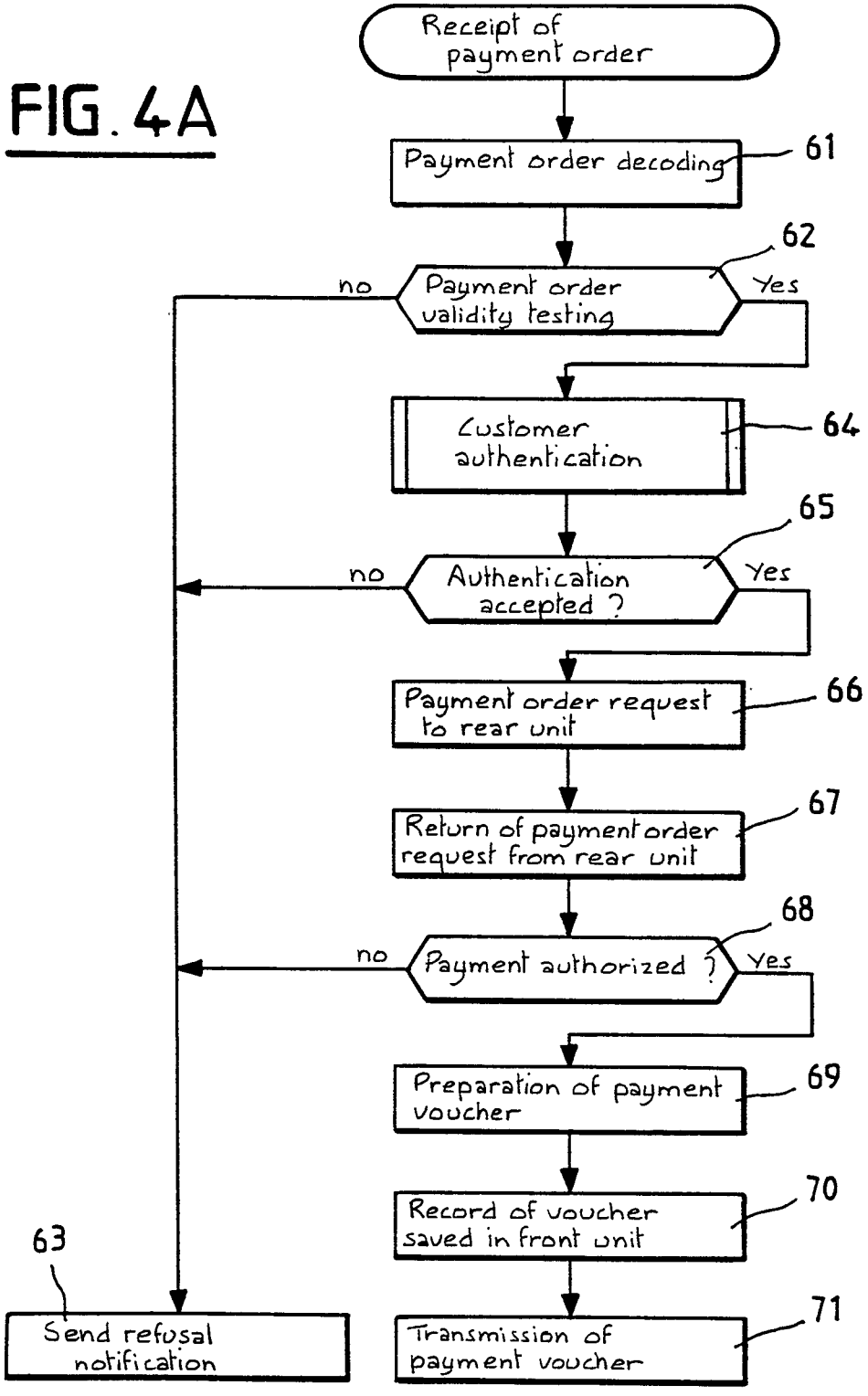
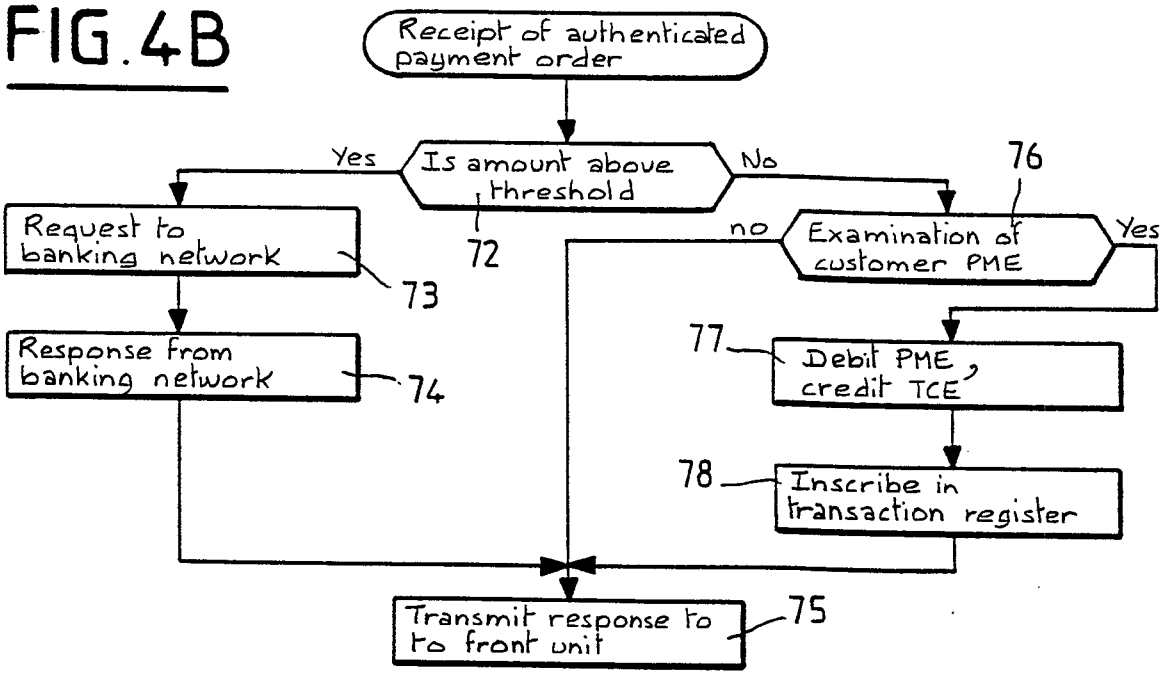

Receipt of payment order
Payment order decoding
61
Payment order validity testing
62
no
Yes
Customer authentication
64
Authentication accepted ?
65
no
Yes
Payment order request to rear unit
66
Return of payment order request from rear unit
67
Payment authorized ?
68
no
Yes
Preparation of payment voucher
69
Record of voucher saved in front unit
70
Transmission of payment voucher
71
63
Send refusal notification

FIG.4B


Receipt of authenticated payment order
Is amount above threshold
Yes
No
72
Request to banking network
73
Response from banking network
74
76
Examination of customer PME
no
Yes
77
Debit PME, credit TCE
78
Inscribe in transaction register
Transmit response to to front unit
75

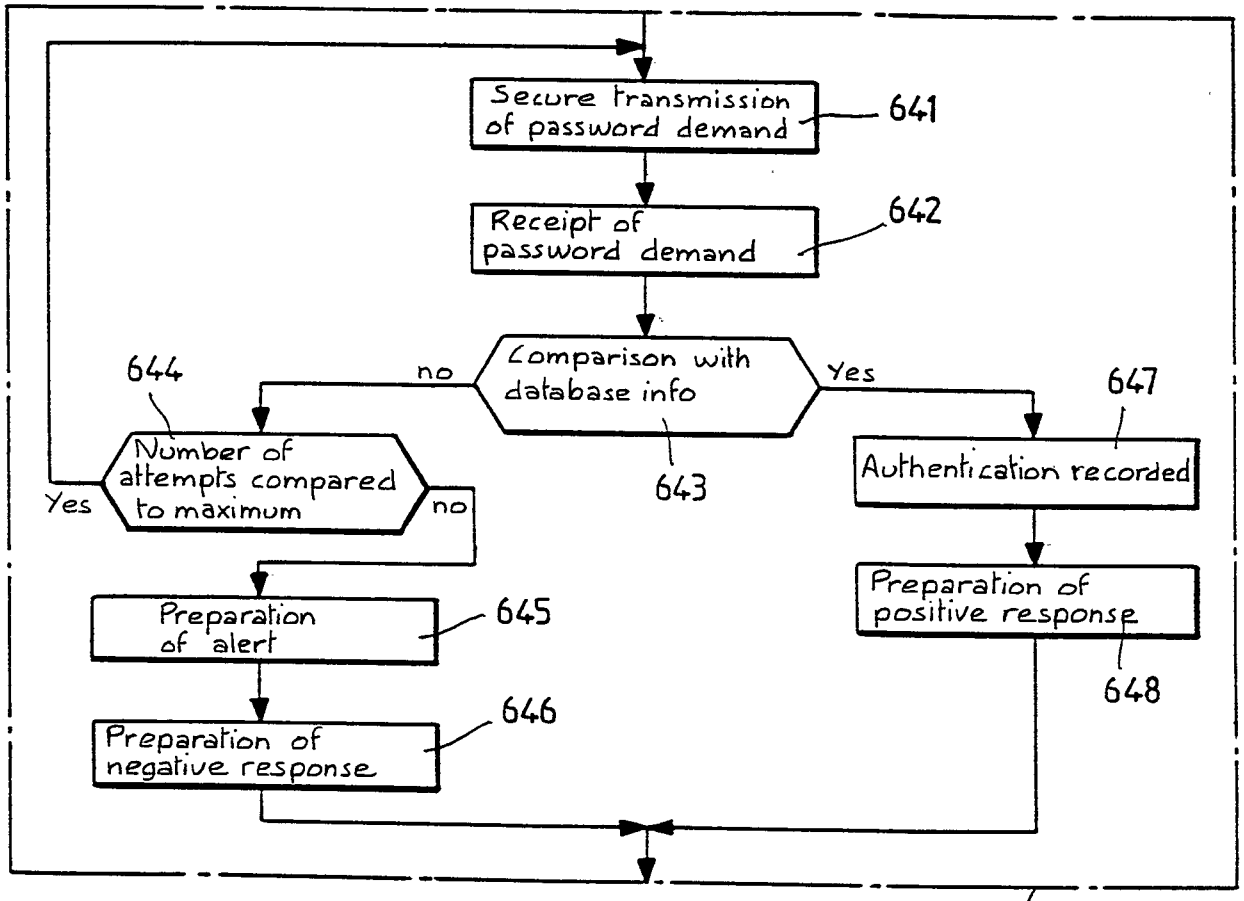
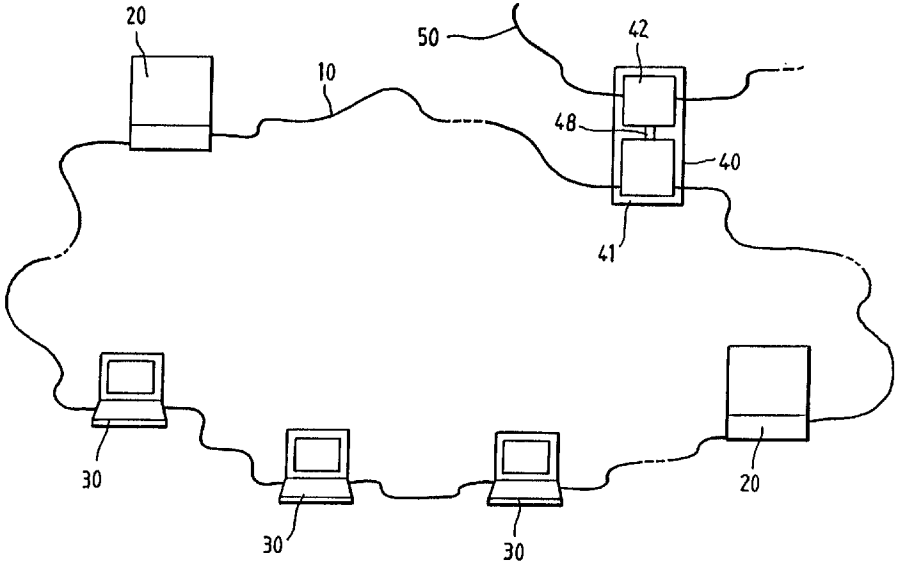

Secure transmission of password demand
641
Receipt of password demand
642
Comparison with database info
no
Yes
643
644
Number of attempts compared to maximum
Yes
no
Preparation of alert
645
Preparation of negative response
646
647
Authentication recorded
Preparation of positive response
648
64

FIG.4C


20
10
50
42
48
40
41
30
30
30
20