Procédé de paiement électronique permettant d'effectuer des transactions liées à l'achat de biens sur un réseau informatique

La présente invention concerne un procédé de paiement électronique permettant d'effectuer des transactions liées à l'achat de biens offerts par des marchands au moyen de services télématiques via un réseau de télécommunication informatique ouvert sur lequel sont connectés des postes serveurs de marchands et des postes clients.

Par réseau informatique ouvert, on entend ici un réseau sur lequel des particuliers ou des entreprises peuvent librement se connecter à la condition de disposer d'une adresse, par exemple le réseau "Internet". Les biens concernés sont des produits ou des services, dont la fourniture est réalisée hors du réseau après la conclusion de la transaction, ou des biens immatériels, tels que des informations, dont la fourniture peut être réalisée via le réseau informatique.

Divers procédés de paiement électronique ont été proposés, certains étant déjà opérationnels.

Plusieurs procédés sont fondés sur une nouvelle représentation de la monnaie. Il s'agit d'une représentation électronique, quelquefois dénommée "jeton" qui peut être purement logicielle ou partiellement matérielle, par exemple avec une carte à puce. Ces procédés impliquent la circulation de monnaie sur le réseau informatique, ce qui pose des problèmes difficiles de sécurité vis-à-vis de la création de fausse monnaie.

D'autres procédés connus de paiement électronique impliquent une relation directe avec une banque ou un réseau bancaire. Typiquement, de tels procédés sont employés dans les réseaux de carte de crédit comme, par exemple, des procédés bien connus utilisant des terminaux points de vente reliés à un circuit carte bancaire ainsi que des procédés utilisant des chèques électroniques avec une signature électronique pour l'authentification de l'acheteur. C'est une forme de lettre d'engagement émise par un acheteur, remise au vendeur et acceptée et reconnue par une banque.

Les procédés qui impliquent à un moment ou un autre de la transaction une relation avec le système bancaire traditionnel et la mise en oeuvre d'une transaction dans ce système présentent des inconvénients. Ainsi, les transactions dans le système bancaire ont un coût réel qui devient prohibitif lorsque le montant de l'achat est très faible, par exemple un montant associé à la consultation d'une base de données. Or, les réseaux informatiques sont bien adaptés à la vente de

biens de faible valeur, principalement des biens d'information, puisque la livraison du bien peut se faire par le réseau lui-même. En outre, l'accès à un réseau bancaire ou un réseau de carte bancaire doit être hautement protégé, ce qui exclut pratiquement la possibilité d'un accès à travers un réseau informatique ouvert, tel que le réseau "Internet" sur lequel des acheteurs potentiels peuvent se connecter.

L'invention a pour but de fournir un procédé permettant d'éviter les inconvénients des procédés connus, en particulier un procédé permettant, sans circulation de monnaie électronique, de réaliser de façon simple et fiable des transactions liées à l'achat de biens sur un réseau informatique, et ce aussi bien pour des biens de prix élevé nécessitant une autorisation par le système bancaire traditionnel, que pour des biens de faible ou très faible prix.

Ce but est atteint grâce à un procédé du type défini en tête de la présente description et comportant, conformément à l'invention, les étapes de :

- élaboration par un poste serveur de marchand connecté au réseau d'une demande d'autorisation de transaction, ou "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,
- transmission du ticket de paiement via le réseau informatique à un poste serveur de paiement distinct des postes clients et serveurs de marchands,
- vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, la vérification étant effectuée, selon le montant du prix à payer, soit par interrogation d'un compte propre au client, tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par interrogation sur un réseau bancaire indépendant du réseau informatique, pour les paiements de montants plus élevés,
- si la vérification est positive, élaboration par le serveur de paiement d'une autorisation de transaction ou bon de caisse comportant au moins une partie des informations du ticket de paiement, et
- transmission du bon de caisse au serveur de marchand via le réseau informatique, afin d'autoriser la réalisation de l'achat.

Ainsi, le procédé selon l'invention est remarquable en ce qu'il n'implique ni la création de monnaie électronique, ni la circulation de monnaie électronique sur le réseau informatique.

La gestion des transactions est effectuée par un serveur de paiement qui seul peut accéder à un réseau bancaire ou un réseau de carte bancaire, et qui

gère des comptes clients non bancaires sur lesquels des transactions de faibles montants peuvent être effectuées.

Le serveur de paiement gère également des comptes marchands non bancaires utilisés pour les transactions de faibles montants. Ainsi, lorsqu'un bon de caisse est transmis après vérification par interrogation d'un compte client tenu par le serveur de paiement, le montant de l'achat est débité du compte client et crédité sur un compte marchand propre au marchand concerné et tenu par le serveur de paiement, ce qui n'entraîne pas des coûts de traitement élevés.

Chaque client dispose d'une identité qui lui est propre pour pouvoir utiliser le procédé de paiement. Il doit également disposer d'un compte bancaire réel, de préférence un compte utilisable au moyen du système traditionnel des cartes bancaires. La vérification par le serveur de paiement peut comprendre une phase préalable de validation de l'identité du client à partir du contenu du ticket de paiement. La validation de l'identité est une opération préalable à l'accès éventuel au compte du client, si le montant de l'achat est faible, et/ou à l'accès au réseau bancaire si le montant est plus élevé. Le serveur de paiement comporte de préférence des moyens, par exemple une base de données, permettant de mémoriser les relations entre les identités des clients utilisées pour les transactions sur le réseau informatique et des identités bancaires (numéros de comptes bancaires ou numéros de cartes de crédit) utilisées pour les transactions sur le réseau bancaire. On peut éviter de la sorte la circulation d'identités bancaires sur le réseau informatique.

Un mode de réalisation de l'invention sera maintenant décrit à titre indicatif, mais non limitatif, en référence aux dessins annexés sur lesquels :

- la figure 1 est une vue générale très schématique d'un système de paiement électronique conforme à l'invention ;
- la figure 2 est une représentation sous forme d'un schéma bloc d'un serveur de paiement du système de la figure 1 ;
- la figure 3 illustre le déroulement des opérations relatives à un achat au moyen du système de la figure 1 ; et
- les figures 4A à 4C sont des organigrammes montrant très schématiquement les opérations effectuées par le serveur de paiement.

Sur la figure 1 est représenté de façon très schématique un réseau de télécommunication informatique 10 sur lequel sont connectés des postes serveurs de marchands 20, des postes clients 30 et au moins un poste serveur de paiement 40.

Le réseau informatique 10 est un réseau ouvert ou public, par exemple le réseau dénommé "Internet".

Les serveurs de marchands 20 sont des unités telles que celles couramment utilisées pour des serveurs télématiques connectés sur "Internet", par exemple des unités organisées autour de machines "Unix" multiprocesseurs.

Les postes clients 30 sont essentiellement des micro-ordinateurs qui sont munis de moyens de connexion au réseau "Internet" 10, par exemple sous forme d'interface "Web". Les serveurs de marchands 20 et de postes clients 30 utilisent par exemple des logiciels connus sous la dénomination "World Wide Web" (WWW) utilisant le protocole HTTP.

Le serveur de paiement 40, montré avec plus de détails sur la figure 2, comprend des unités frontale et dorsale respectivement 41 et 42 connectées toutes les deux au réseau "Internet" 10. L'unité frontale 41 a une architecture semblable à celle d'un serveur classique connecté sur un réseau tel qu'"Internet"". L'unité dorsale 42 comporte une unité de traitement 43 à un ou plusieurs processeurs, une base de données 44 comportant des informations relatives aux marchands et clients abonnés au système de paiement, un registre de transactions 45, une unité 46 d'interface avec un réseau bancaire ou un réseau de carte bancaire 50, et un bus de communication 47 ou autre liaison similaire permettant de relier entre eux les différents constituants de l'unité dorsale 42. Une liaison sécurisée 48 permet une communication bidirectionnelle entre l'unité frontale 41 et l'unité de traitement 43. La communication avec le réseau informatique 10 est contrôlée par l'unité frontale 41 tandis que la gestion de la base de données 44 ainsi que le contrôle de la communication avec le réseau bancaire 50 sont assurés par l'unité dorsale 42.

La base de données 44 contient des informations relatives aux clients et aux marchands abonnés au système de paiement. Pour chaque client, la base de données 44 contient l'identité système du client ("CId"), identité reçue lors de l'abonnement au système, un compte de client ou porte monnaie électronique ("PME") destiné au paiement de faibles montants, une identité bancaire telle que numéro de compte bancaire réel ou numéro de carte de crédit ainsi qu'éventuellement une clef d'accès ou mot de passe propre au client. Pour chaque marchand, la base de données 44 contient l'identité système du marchand ("MId"), identité reçue lors de l'abonnement au système, un compte de marchand, ou tiroir-caisse électronique ("TCE") destiné à l'encaissement des faibles montants et une identité bancaire telle que numéro de compte bancaire réel.

La figure 3 illustre schématiquement les différentes étapes d'une transaction portant sur un achat d'un bien par un client abonné à un marchand abonné. Il peut s'agir d'un bien matériel dont la livraison au client sera effectuée réellement après conclusion de la transaction ou d'un bien immatériel (tel que de l'information) qui peut être fournie au client par le réseau informatique dès le paiement électronique effectué.

(1) Consultation par le client

Par connexion sur le réseau "Internet" 10, un client peut consulter en ligne le catalogue ou la "vitrine" d'un marchand quelconque par accès au serveur 20 du marchand et par visualisation sur l'écran du poste client 30 des biens ou services du marchand. Sur présentation de l'identité CId du client, le serveur du marchand peut présenter au client des conditions financières particulières (par exemple une remise) applicables à la transaction éventuelle.

(2) Demande d'achat

Le choix du client étant arrêté sur un bien O, il est transmis au serveur du marchand sous forme d'un message contenant une identité OId du bien et l'identité CId du client. Lorsque cela est nécessaire, par exemple pour la livraison ultérieure du bien choisi, des informations complémentaires (par exemple une adresse et un horaire de livraison préféré). Cela peut être réalisé de façon commode en utilisant un formulaire électronique envoyé sur le réseau et destiné à être rempli par le client.

Dans le cas où l'achat envisagé représente un montant élevé ou est soumis à des conditions légales, une authentification préalable du client peut être souhaitée. Comme on le verra en détail plus loin l'authentification d'un client est effectuée par le serveur de paiement 40. Aussi, une demande d'authentification provenant d'un marchand est émise avantageusement sous la forme d'un ticket de paiement de valeur nulle qui est transmis au serveur de paiement par le réseau informatique via le poste client et, en cas d'authentification positive, provoque le retour d'un bon de caisse du serveur de paiement au serveur marchand, toujours via le poste client. Les procédures d'établissement d'un ticket de paiement et de renvoi d'un bon de caisse sont décrites plus en détail ci-après.

La demande d'achat émise par le client peut porter sur un seul bien ou sur plusieurs biens à fournir de façon groupée : "achat panier".

(3) Elaboration de la demande de paiement

En réponse à une demande d'achat, le serveur marchand élabore une demande de paiement qui peut comprendre les informations suivantes :

- Identité du marchand, ("MId");
- Description du bien commandé, ou de chacun des biens du panier, en cas d'achats groupés;
- Type de transaction (simple ou panier);
- Identité du client, ("CId");
- Identité du bien ou de l'ensemble des biens du panier, ("OId");
- Prix de l'objet, ("Oid");
- TVA (si applicable);
- Date et heure de l'émission du ticket de paiement (horodatage par le serveur marchand);
- Durée de validité du ticket de paiement;
- Numéro de série dans le registre des ventes du marchand (notamment dans le cas où la transaction a comporté une étape préalable d'authentification).

L'ensemble des informations ci-dessus est encodée dans une chaîne d'octets qui constitue la chaîne opaque d'un ticket de paiement (ou URL de commande de bien, URL étant les initiales de "Uniform Resource Locator" ou Localisateur de Ressource Uniforme utilisé dans les logiciels WWW avec protocole HTTP), comme suit:

URL http : < SP> < descriptif de la commande> ,

où SP est l'adresse "Internet" du serveur de paiement. Le ticket de paiement est adressé au poste client. Il est complété par deux "ancres" logiques qui permettent au client soit de l'annuler, soit de le confirmer.

(4) Envoi de l'ordre de paiement

L'ordre de paiement est transmis au serveur de paiement simplement par validation par le client de l'URL de demande de paiement. On comprendra bien que le ticket de paiement ne fait alors que transiter par le poste client.

(5) Emission du bon de caisse

Sur réception d'un ordre de paiement, le serveur de paiement 40 le décode et procède à l'authentification du client et recherche si le paiement peut être autorisé avant de retourner un bon de caisse ou un refus de paiement.

Les opérations d'authentification de client et d'autorisation de paiement seront décrites plus loin en détail en référence à la figure 4.

Lorsque les vérifications effectuées ne permettent pas d'autoriser le paiement, une notification de refus motivée est adressée au client par le serveur de paiement (indiquant, par exemple, compte insuffisamment approvisionné, dépassement d'un seuil autorisé pour le client, ...)

Lorsque les vérifications effectuées permettent d'autoriser le paiement, les informations contenues dans le ticket de paiement sont complétées avec un numéro de série dans le registre des transactions 45, une estampille horaire, une durée de validité (typiquement quelques dizaines de secondes) et le sceau du serveur de paiement constituant une information de certification. L'ensemble de ces informations, éventuellement après signature numérique par l'utilisation de la partie de clef privée d'un système de chiffrement à clef privée/clef publique du serveur de paiement (ce qui garantit la validité et l'intégrité de l'autorisation de paiement), est encodé dans une chaîne d'octets qui constitue la chaîne opaque d'un bon de caisse ou URL de livraison :

URL http : <M> <descriptif du bon de caisse> ,

où <M> est l'adresse "Internet" du marchand.

(6) Demande de livraison

Le bon de caisse est transmis au serveur du marchand via le poste client. Ceci peut être effectué automatiquement par le logiciel implanté au poste client en utilisant la possibilité de re-routage des URL bien connue de l'homme du métier. Avant d'autoriser la livraison du bien, le serveur du marchand opère un décodage et une vérification du bon de caisse reçu. Cette vérification consiste à utiliser la clef privée éventuelle du serveur de paiement, à vérifier que la durée de validité n'est pas écoulée, et à rapprocher le contenu du bon de caisse avec celui de la demande de paiement.

(7) Livraison du bien

Lorsque le bon de caisse est validé par le serveur du marchand, celui-ci peut effectuer la livraison directe sur le poste client, dans le cas de bien d'information, ou adresse au poste client un document permettant le retrait du bien et précisant notamment le lieu de livraison et le nom du récipiendaire.

On notera que, dans le cas d'un achat groupé (panier), il y a création par le serveur du marchand d'un objet avec affectation d'une identité unique. Cet objet est la liste des URL de chacun des biens du panier. C'est cet objet qui est indiqué dans l'URL de commande de bien et qui permettra d'enregistrer le détail des biens achetés dans le registre de transaction du serveur de paiement.

Les figures 4A à 4C montrent les opérations effectuées par le serveur de paiement 40 en réponse à la réception d'un ordre de paiement.

Dans l'unité frontale 41 (figure 4A), l'ordre de paiement est décodé (étape 61) et sa validité est examinée (test 62) notamment du point de vue de la

durée de validité. Si le résultat de l'examen est négatif, une notification de refus est envoyée au poste client (étape 63).

Si le résultat de l'examen est positif, il est procédé ensuite à une authentification du client (étape 64), le détail de cette opération étant décrit plus loin en référence à la figure 4C. Si l'authentification est négative (test 65), une notification de refus est envoyée au client (étape 63). Si elle est positive, l'ordre de paiement (éventuellement limité à l'identité CId du client, à l'identité MId du marchand, et au prix) est transmis via la liaison 68 à l'unité dorsale 42 du serveur de paiement représenté sur la figure 2 (étape 66). La liaison 48 est une liaison sécurisée interdisant l'accès à l'unité dorsale à toute personne se connectant sur le réseau 10.

L'unité frontale 41 attend alors que l'unité dorsale décide d'autoriser ou non le paiement (étape 67). Si le paiement n'est pas autorisé, (test 68), une notification de refus est envoyée au poste client (étape 63). Si le paiement est autorisé, un bon de caisse est élaboré (étape 69), utilisant les informations enregistrées à l'étape 62. Le bon de caisse est enregistré dans une mémoire de l'unité frontale 41 (étape 70) et est adressé au serveur du marchand via le poste client (étape 71).

Au niveau de l'unité dorsale 42 (figure 4B) du serveur de paiement, à la réception d'un ordre de paiement authentifié, il est examiné si celui-ci doit être autorisé à partir du compte client PME via le réseau bancaire 50. A cet effet, le prix est comparé à un seuil minimum (test 72). Ce seuil est par exemple de quelques dizaines de francs.

Si le seuil est dépassé, une demande pour effectuer l'opération de paiement est lancée sur le réseau bancaire (étape 73) en utilisant l'identité bancaire correspondant à l'identité CId du client, telle qu'elle ressort de la consultation de la base de données 44. A la réception de la réponse positive ou négative (étape 74), celle-ci est transmise à l'unité frontale 41 (étape 75).

Si le seuil n'est pas dépassé, le paiement peut être effectué à partir du compte PME du client.

A cet effet, il est examiné si le compte est suffisamment approvisionné (test 76). Dans la négative, un refus d'autorisation de paiement, c'est-à-dire une réponse négative, est renvoyée à l'unité frontale (étape 75). Dans l'affirmative, le compte PME du client est débité du prix et le compte TCE de marchand correspondant à l'identité MId est crédité du même montant (étape 77), la transaction est inscrite dans le registre des transactions 45 (étape 78) et

l'autorisation de paiement, c'est-à-dire une réponse positive est transmise à l'unité frontale 41 avec l'indication du numéro de série de l'inscription dans le registre de transactions (étape 75).

La procédure d'authentification dans le serveur de paiement (figure 4C), à l'étape 64 de la figure 4A, comprend l'envoi au poste client, de préférence dans une forme sécurisée (chiffrée), d'une demande de clé d'accès, ou mot de passe (étape 641). A la réception sécurisée de la clé d'accès (étape 642), une comparaison est effectuée avec une information correspondante contenue dans la base de données 44 (test 643).

Si la comparaison est négative, et qu'un nombre maximum de tentatives infructueuses n'a pas été atteint (test 644), on retourne à l'étape 641. Si ce nombre maximum est atteint, l'absence d'authentification est constatée, une alerte est produite (étape 645) et une réponse négative est envoyée au poste client (étape 646). L'alerte peut consister en une annulation du compte PME ou en une surveillance de celui-ci afin de détecter de nouvelles tentatives d'utilisation. Si le test à l'étape 643 est positif, l'authentification est enregistrée (étape 647) et une réponse positive est élaborée (étape 648).

Des techniques de chiffrement permettant la transmission sécurisée d'informations numériques sur réseau informatique, notamment pour la demande d'envoi de clé d'accès et l'envoi de celle-ci, sont bien connues.

La procédure d'authentification décrit ici permet d'effectuer une authentification préalable d'un client dans le cas où celle-ci est nécessaire avant l'établissement d'une demande de paiement par le serveur du marchand. Pour cette authentification, il suffit alors en effet de créer un ticket de paiement dans lequel le prix indiqué est nul, comme indiqué plus haut.

L'enregistrement des bons de caisse dans l'unité frontale permet aux clients et aux marchands de procéder à des contrôles et d'en obtenir éventuellement des copies. L'enregistrement des transactions dans l'unité dorsale permet d'en conserver une trace en cas, par exemple, de contestation entre un client et un marchand.

Les comptes clients PME gérés par le serveur de paiement ont en principe un montant de solde plafonné et, selon le mode de réalisation préféré de l'invention, ils ne sont pas rémunérés (le système de paiement se trouvant en dehors du monde bancaire). Un réapprovisionnement de son compte PME par un client peut être effectué à partir de son compte bancaire, par ordre donné à son établissement bancaire.

Les comptes marchands TCE gérés par le serveur de paiement sont associés à des comptes bancaires réels des marchands dans lesquels ils sont vidés par exemple quotidiennement.

Bien que l'on ait décrit ci-avant un mode de mise en oeuvre d'un procédé selon l'invention dans un environnement "Internet" et avec des logiciels WWW utilisant le protocole HTTP, l'homme de l'art comprendra aisément que le procédé peut être mis en oeuvre avec un réseau informatique autre qu'"Internet" ou encore avec des logiciels serveur marchand et client n'utilisant pas le protocole HTTP de WWW. En outre des procédés d'authentification sécurisés mettant en jeu des dispositifs matériels tels que lecteur de carte à puce ou moyen de reconnaissance d'empreinte vocale pourront être prévus à la place de clefs d'accès. Ces dernières et d'autre modifications qui viendront à l'esprit du l'homme du métier sont comprises dans la philosophie et la portée de la présente invention.

REVENDICATIONS

1. Procédé de paiement électronique pour des transactions liées à l'achat de biens offerts par des marchands à des clients via un réseau informatique ouvert sur lequel sont connectés des postes serveurs de marchands et des postes clients, caractérisé par les étapes de :

– élaboration par un poste serveur de marchand connecté au réseau d'une demande d'autorisation de transaction, ou 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,

– transmission du ticket de paiement via le réseau informatique à un serveur de paiement distinct des postes clients et serveurs de marchands,

– vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, la vérification étant effectuée, selon le montant du prix à payer, soit par interrogation d'un compte client propre au client, tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par interrogation sur un réseau bancaire indépendant du réseau informatique, pour les paiements de montants plus élevés,

– si la vérification est positive, élaboration par le serveur de paiement d'une autorisation de transaction ou bon de caisse comportant au moins une partie des informations du ticket de paiement, et

– transmission du bon de caisse au serveur de marchand via le réseau informatique, afin d'autoriser la réalisation de l'achat.

2. Procédé selon la revendication 1, caractérisé en ce que lorsqu'un bon de caisse est transmis après vérification par interrogation d'un compte client tenu par le serveur de paiement, le montant de l'achat est débité du compte client et crédité sur un compte marchand propre au marchand concerné et tenu par le serveur de paiement.

3. Procédé selon l'une quelconque des revendications 1 et 2, caractérisé en ce que la vérification par le serveur de paiement comprend une phase préalable d'authentification du client.

4. Procédé selon la revendication 3, caractérisé en ce que l'authentification est réalisée par reconnaissance d'une clef d'accès transmise par le réseau informatique du poste client au serveur de paiement.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend l'élaboration par le serveur de paiement d'un bon de caisse

comportant au moins une partie des informations du ticket de paiement et une information de certification.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend la mémorisation par le serveur de paiement des transactions autorisées, par stockage d'au moins une partie du contenu des bons de caisse.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le ticket de paiement est transmis du serveur du marchand au serveur de paiement par l'intermédiaire du poste client.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le bon de caisse est transmis du serveur de paiement au serveur du marchand par l'intermédiaire du poste client.

9. Système de paiement électronique pour effectuer des transactions liées à l'achat de biens offerts par des marchands à des clients via un réseau informatique ouvert, le système comportant des postes clients et des postes serveurs de marchands pouvant être connectés sur le réseau ouvert,
système caractérisé en ce qu'il comporte en outre au moins un poste serveur de paiement distinct des postes clients et serveurs de marchands et comprenant :

– une unité frontale munie de moyens de connexion au réseau ouvert,

– une unité dorsale munie de moyens de connexion à un réseau bancaire indépendant du réseau ouvert,

– des moyens de communication entre les unités frontale et dorsale,

– des moyens de mémorisation de comptes de clients, de comptes de fournisseurs, et

– des moyens de traitement pour, en réponse à la réception par l'unité frontale d'une demande d'autorisation de transaction ou ticket de paiement, concernant un achat envisagé entre un marchand et un client, vérifier si le paiement du prix est autorisé pour le client concerné par interrogation du compte du client ou du réseau bancaire et, si la vérification est positive, élaborer une autorisation de transaction, ou bon de caisse afin de la transmettre sur le réseau ouvert via l'unité frontale.

10. Système de paiement selon la revendication 9, caractérisé en ce que le serveur de paiement comprend des moyens de mémorisation des transactions autorisées.

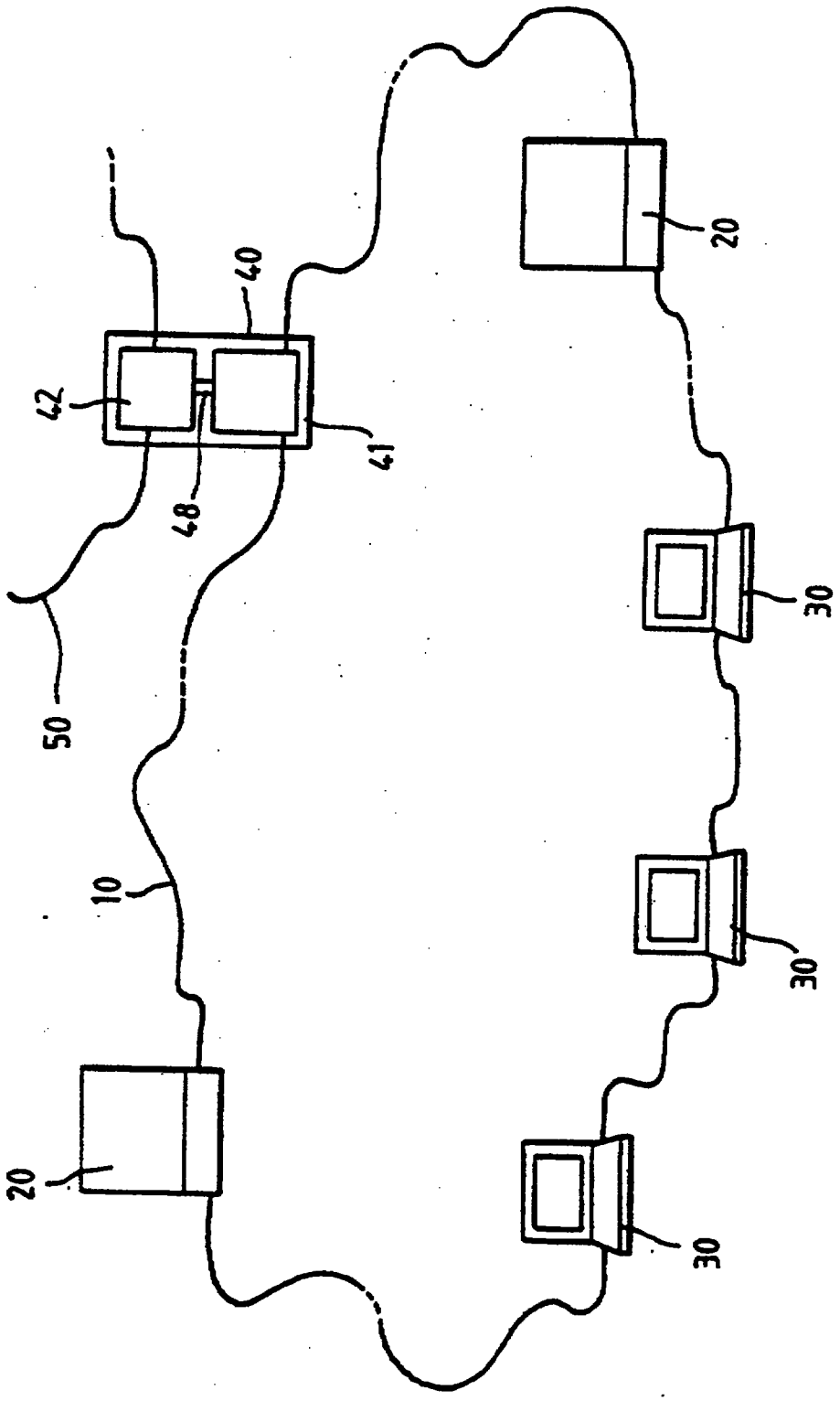


FIG.1

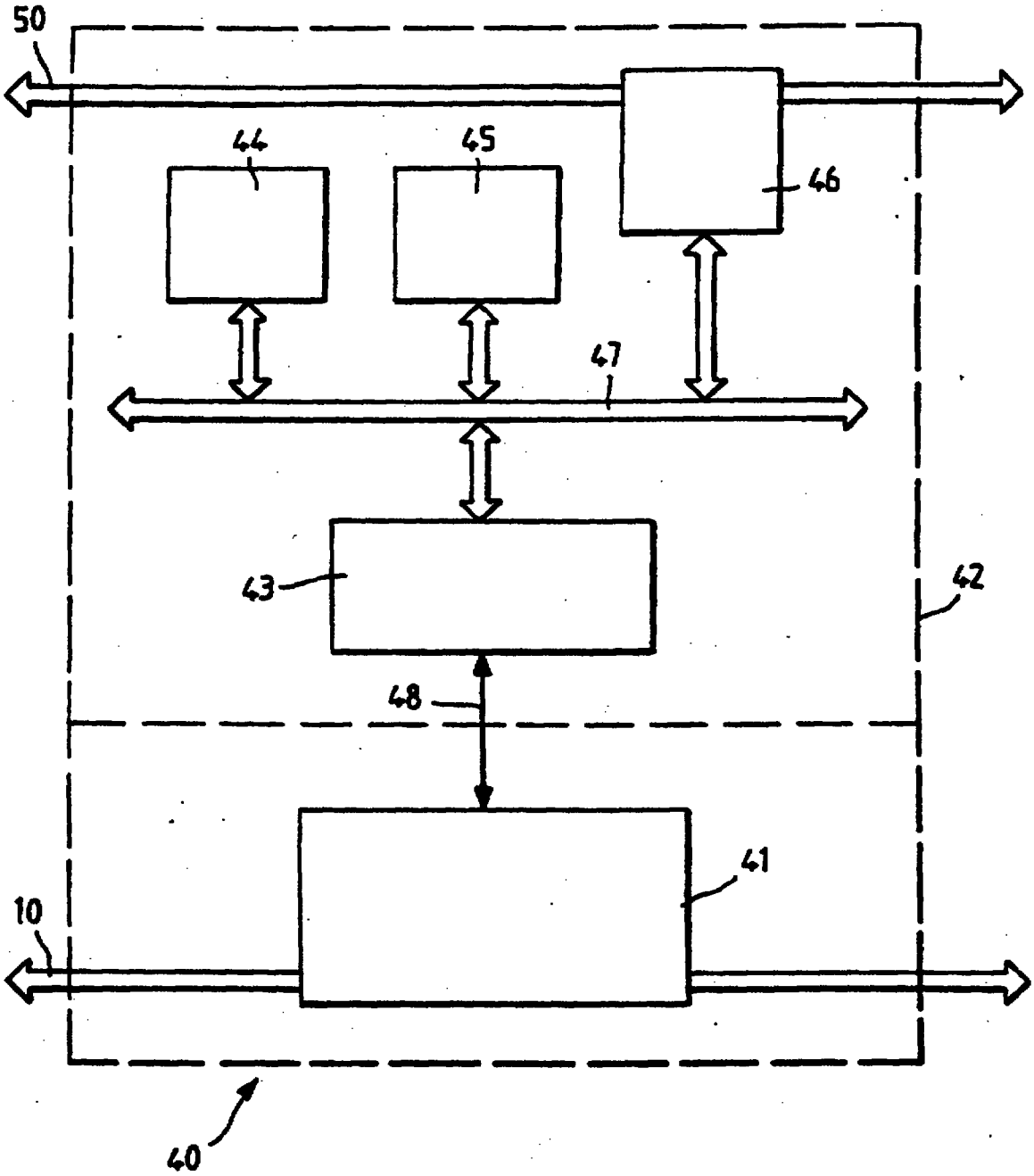


FIG. 2

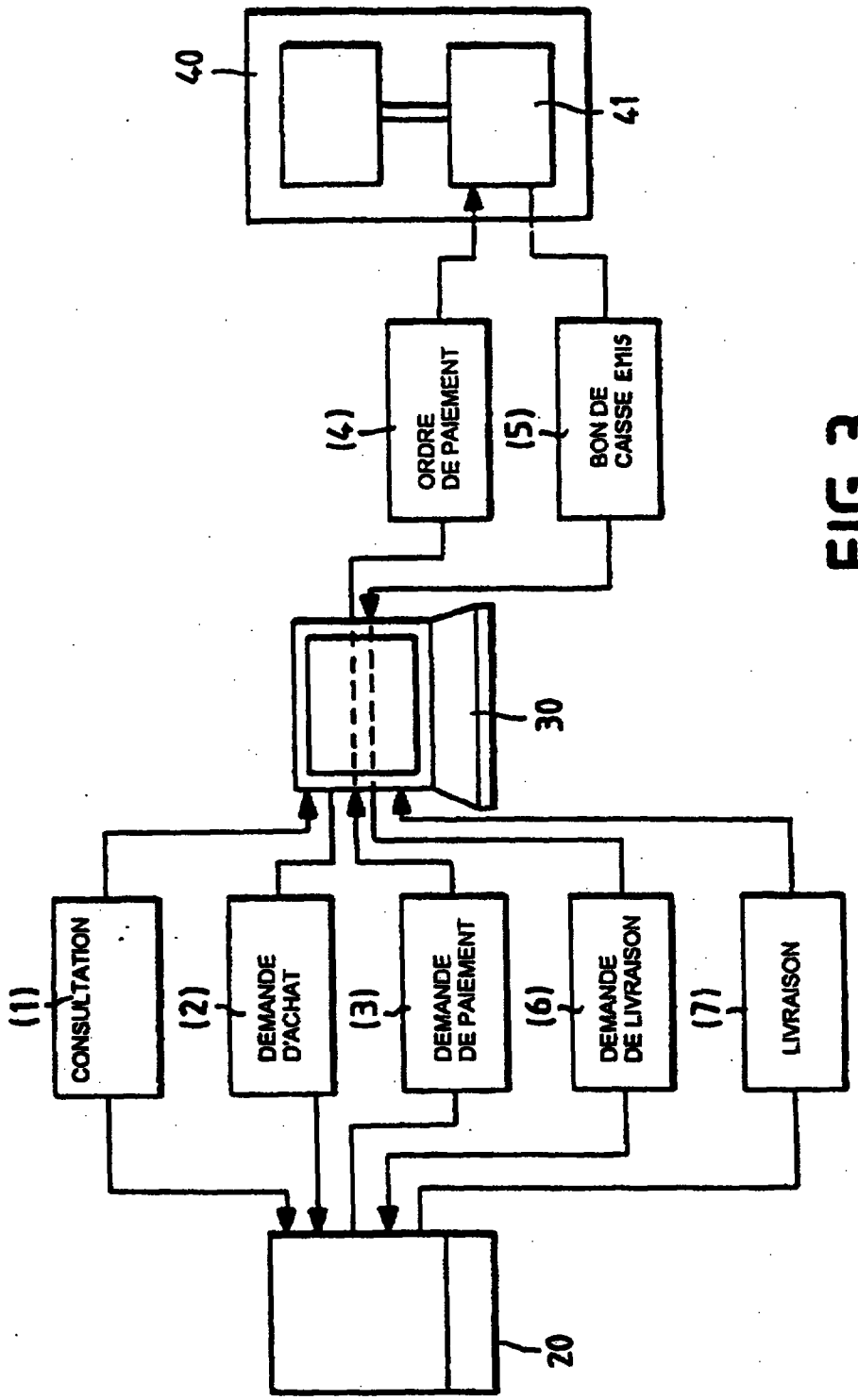

40
41
(4)
ORDRE DE PAIEMENT
(5)
BON DE CAISSE EMIS
30
(1)
CONSULTATION
(2)
DEMANDE D'ACHAT
(3)
DEMANDE DE PAIEMENT
(6)
DEMANDE DE LIVRAISON
(7)
LIVRAISON
20

FIG.3

FIG. 4A

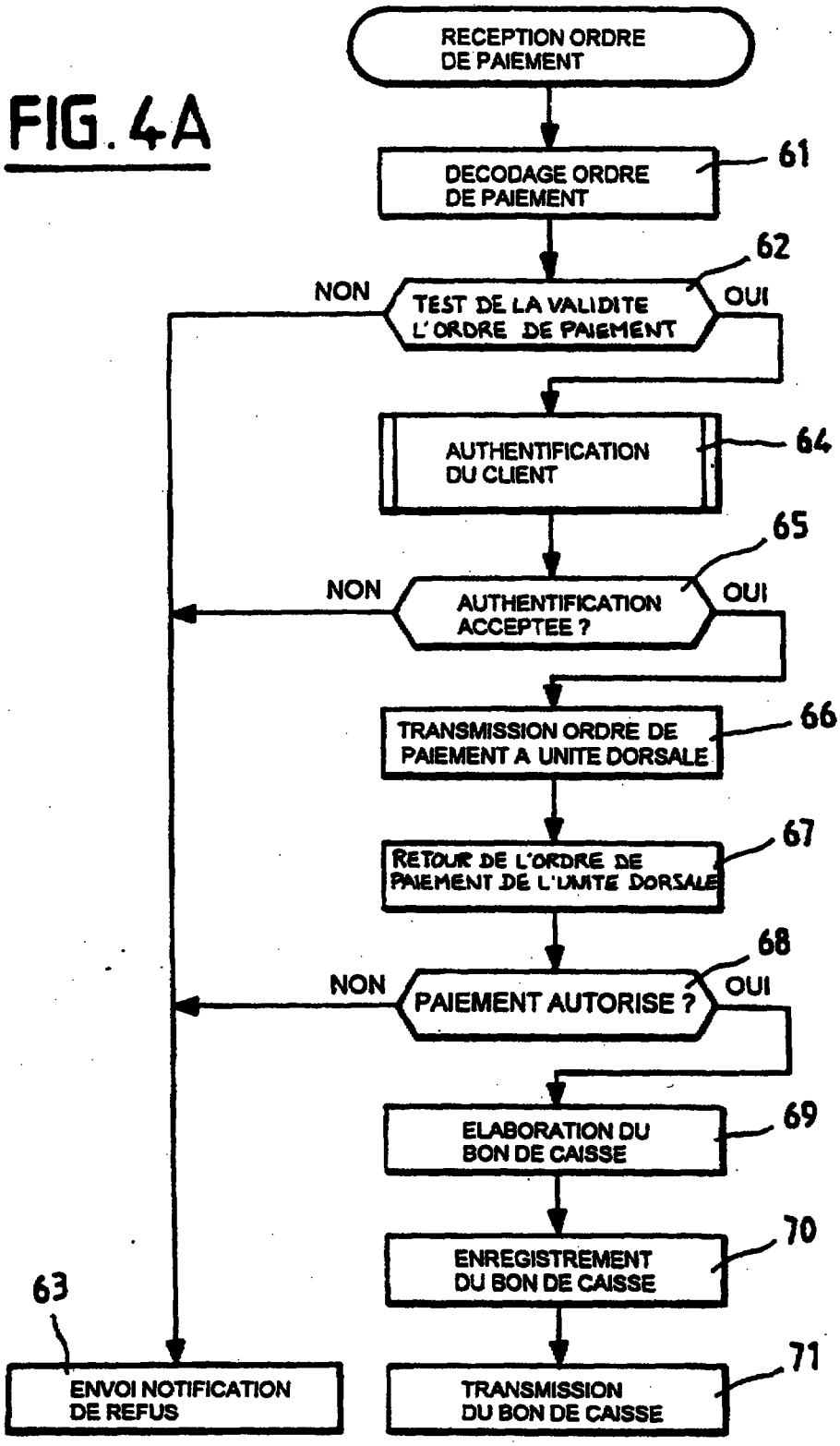
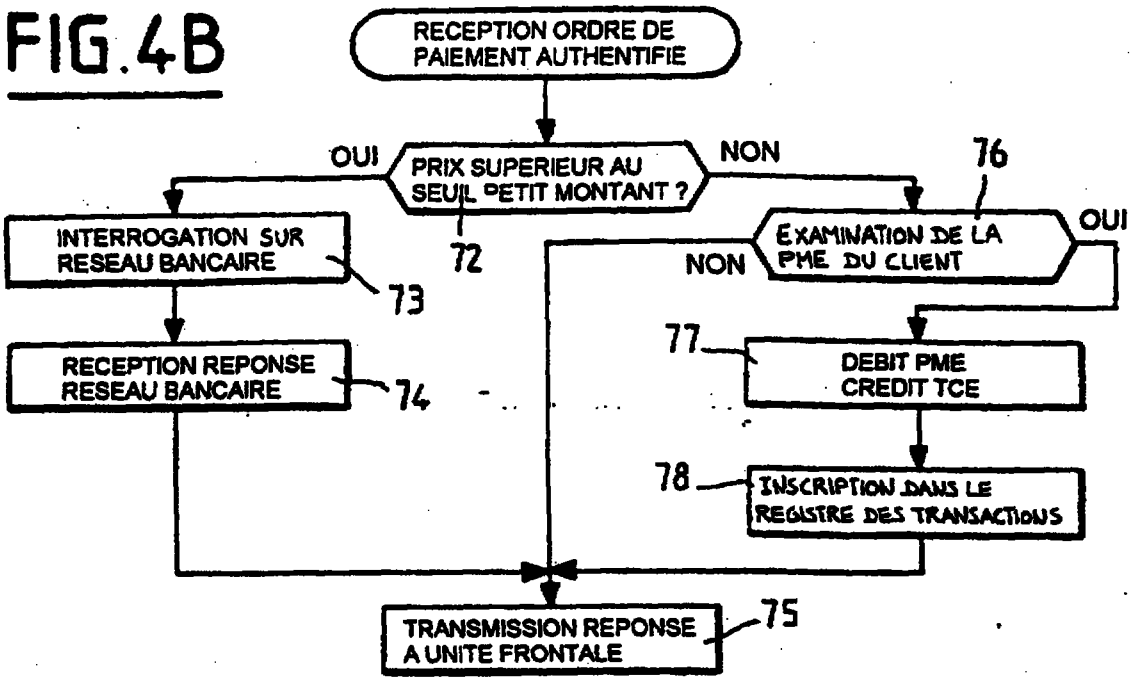

RECEPTION ORDRE DE PAIEMENT
DECODAGE ORDRE DE PAIEMENT
61
TEST DE LA VALIDITE L'ORDRE DE PAIEMENT
62
NON
OUI
AUTHENTIFICATION DU CLIENT
64
AUTHENTIFICATION ACCEPTEE ?
65
NON
OUI
TRANSMISSION ORDRE DE PAIEMENT A UNITE DORSALE
66
RETOUR DE L'ORDRE DE PAIEMENT DE L'UNITE DORSALE
67
PAIEMENT AUTORISE ?
68
NON
OUI
ELABORATION DU BON DE CAISSE
69
ENREGISTREMENT DU BON DE CAISSE
70
TRANSMISSION DU BON DE CAISSE
71
ENVOI NOTIFICATION DE REFUS
63

FIG.4B


RECEPTION ORDRE DE PAIEMENT AUTHENTIFIE
PRIX SUPERIEUR AU SEUIL PETIT MONTANT ?
OUI
NON
72
INTERROGATION SUR RESEAU BANCAIRE
73
RECEPTION REPONSE RESEAU BANCAIRE
74
76
EXAMINATION DE LA PME DU CLIENT
OUI
NON
77
DEBIT PME CREDIT TCE
78
INSCRIPTION DANS LE REGISTRE DES TRANSACTIONS
TRANSMISSION REPONSE A UNITE FRONTALE
75

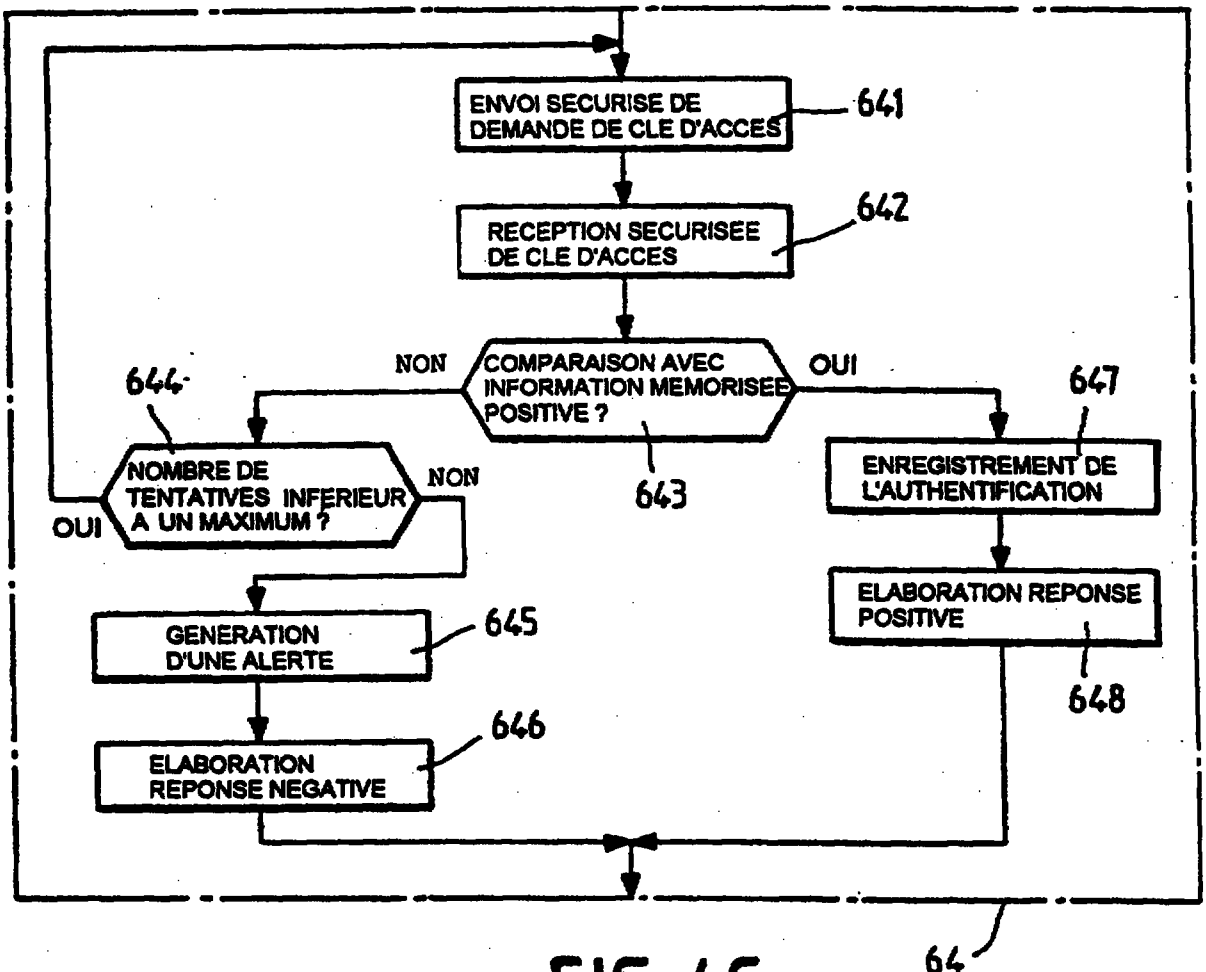

ENVOI SECURISE DE DEMANDE DE CLE D'ACCES
641
RECEPTION SECURISEE DE CLE D'ACCES
642
COMPARAISON AVEC INFORMATION MEMORISEE POSITIVE ?
NON
OUI
643
644
NOMBRE DE TENTATIVES INFERIEUR A UN MAXIMUM ?
NON
OUI
GENERATION D'UNE ALERTE
645
ELABORATION REPONSE NEGATIVE
646
647
ENREGISTREMENT DE L'AUTHENTIFICATION
ELABORATION REPONSE POSITIVE
648
64

FIG.4C

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.

* C L M S *

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

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.

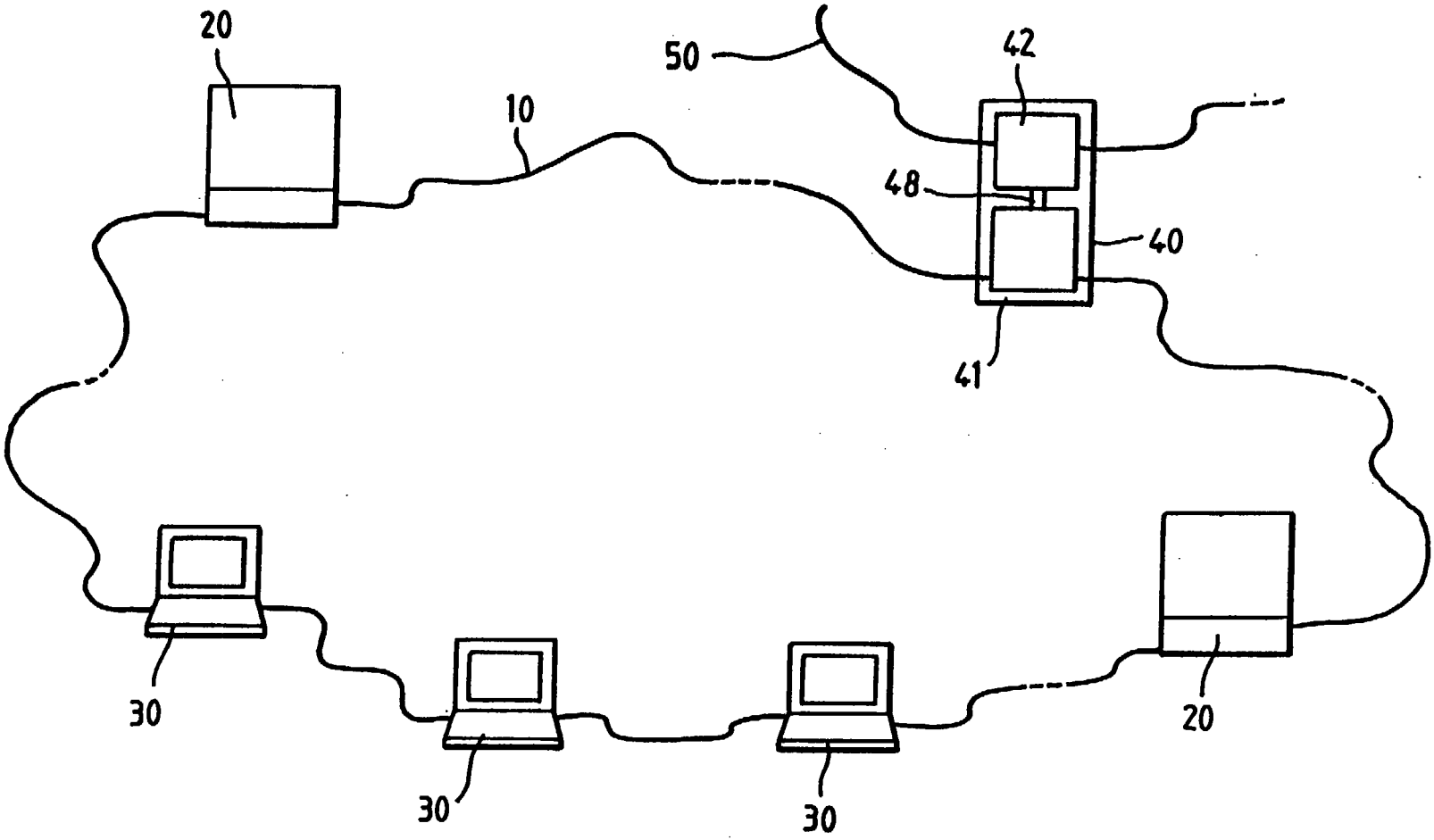


FIG.1

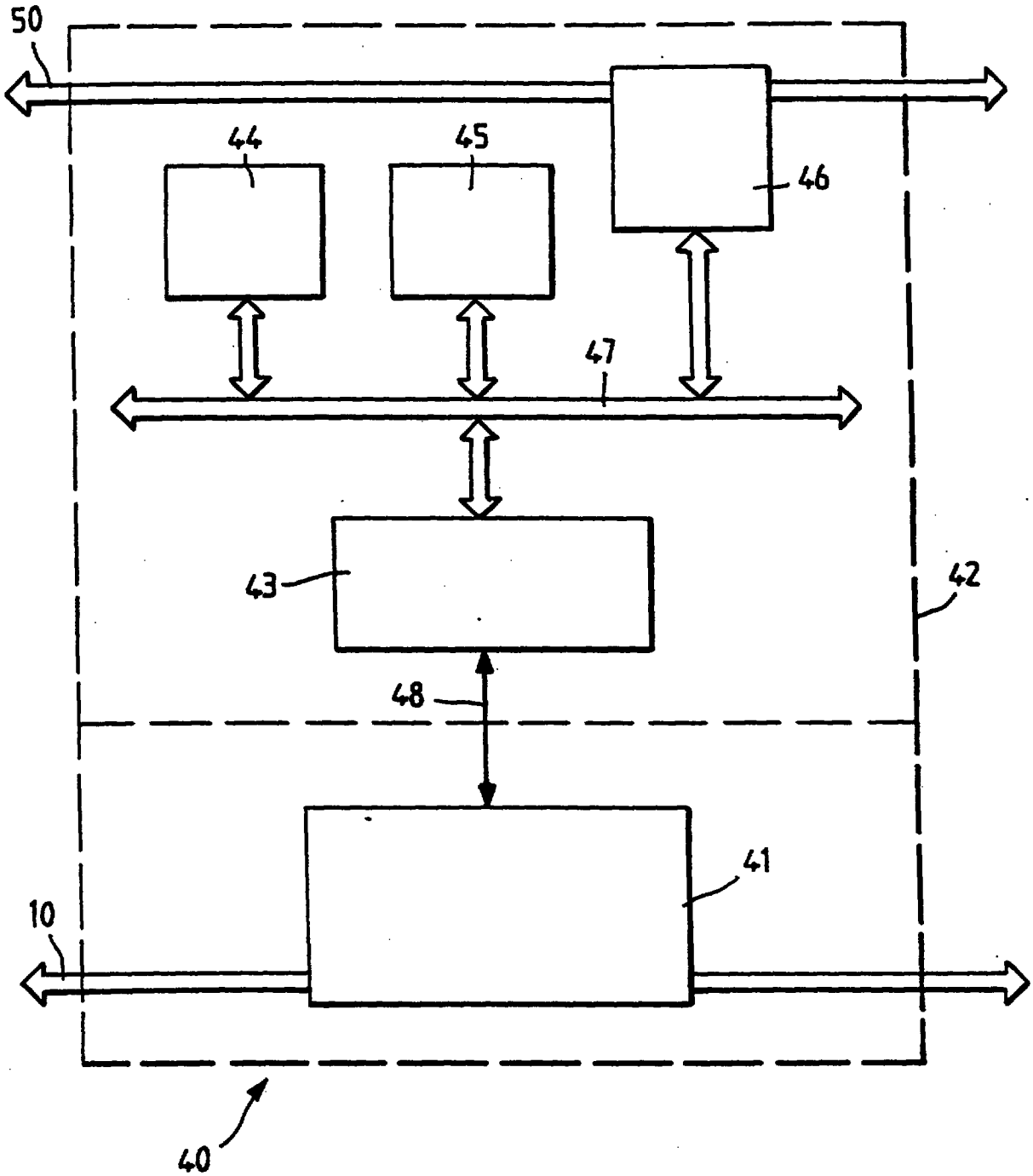


FIG. 2

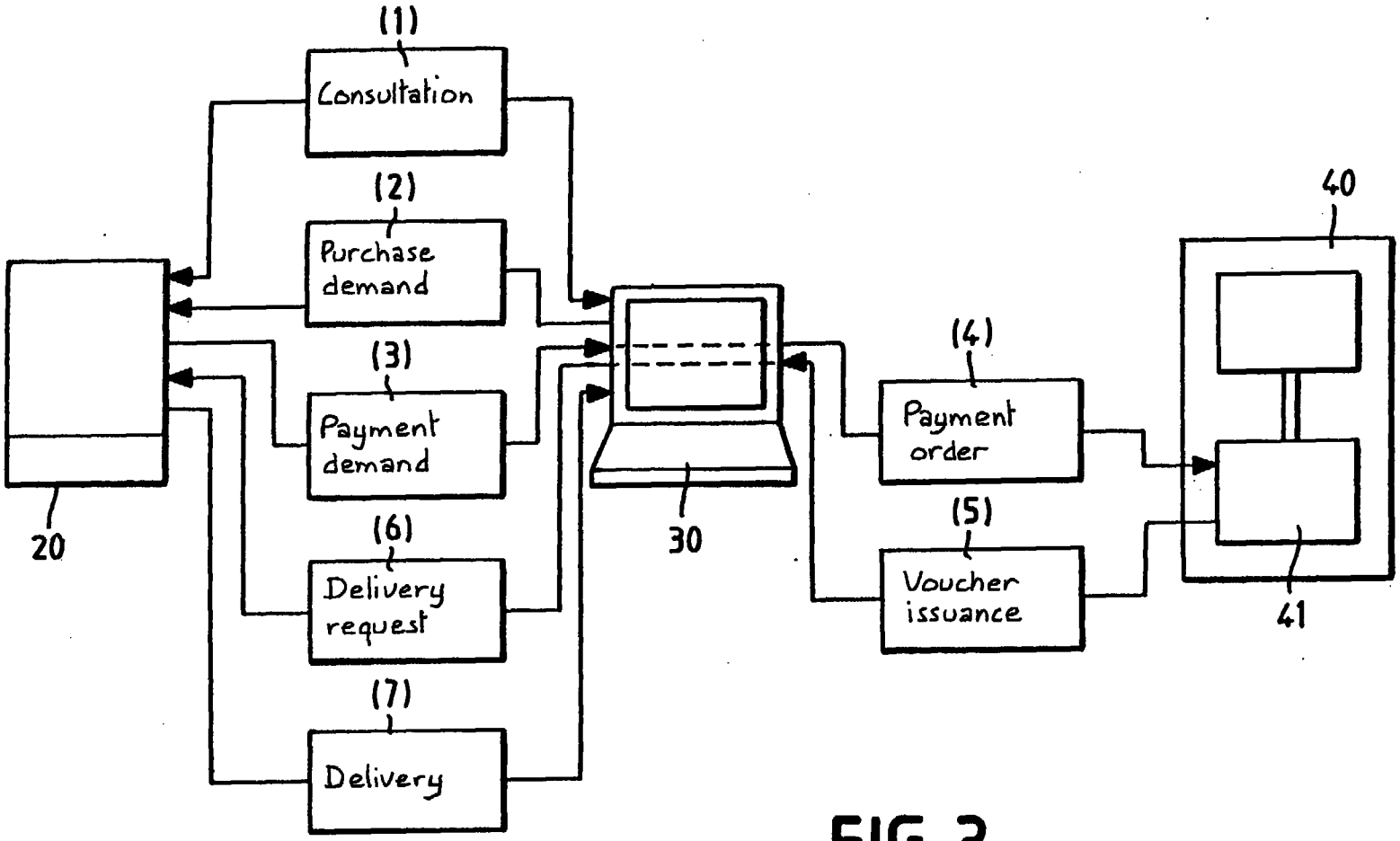

(1)
Consultation
(2)
Purchase demand
(3)
Payment demand
(6)
Delivery request
(7)
Delivery
20
30
(4)
Payment order
(5)
Voucher issuance
40
41

FIG. 3

FIG. 4A

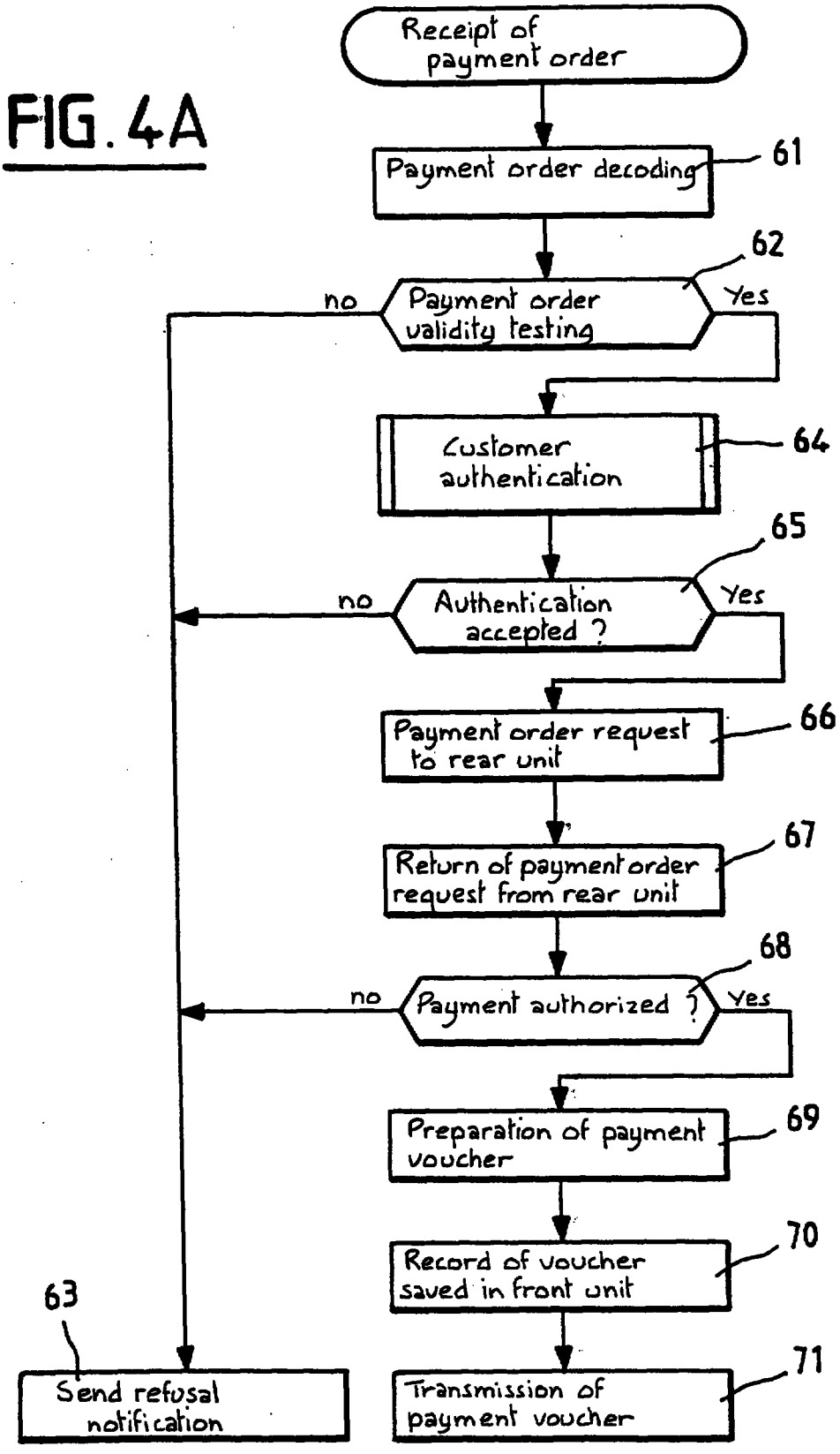
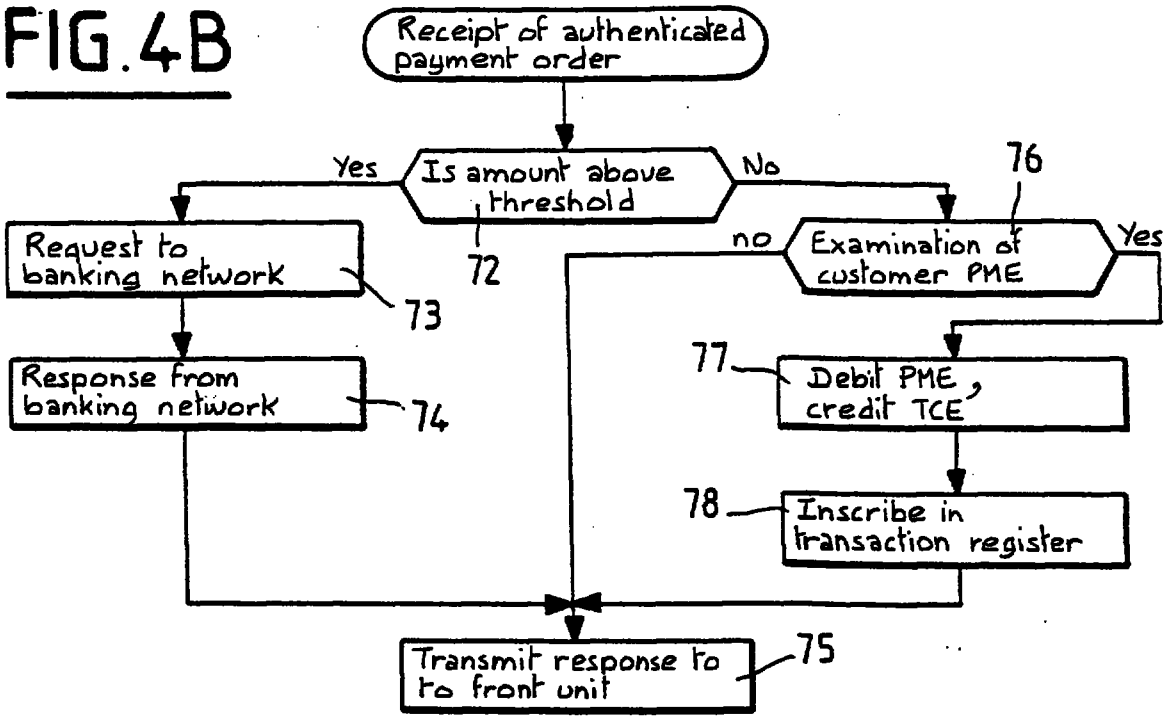

Receipt of payment order
Payment order decoding
61
62
no
Payment order validity testing
Yes
Customer authentication
64
65
no
Authentication accepted ?
Yes
Payment order request to rear unit
66
Return of payment order request from rear unit
67
68
no
Payment authorized ?
Yes
Preparation of payment voucher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

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
no
Examination of customer PME
Yes
77
Debit PME, credit TCE
78
Inscribe in transaction register
Transmit response to to front unit
75

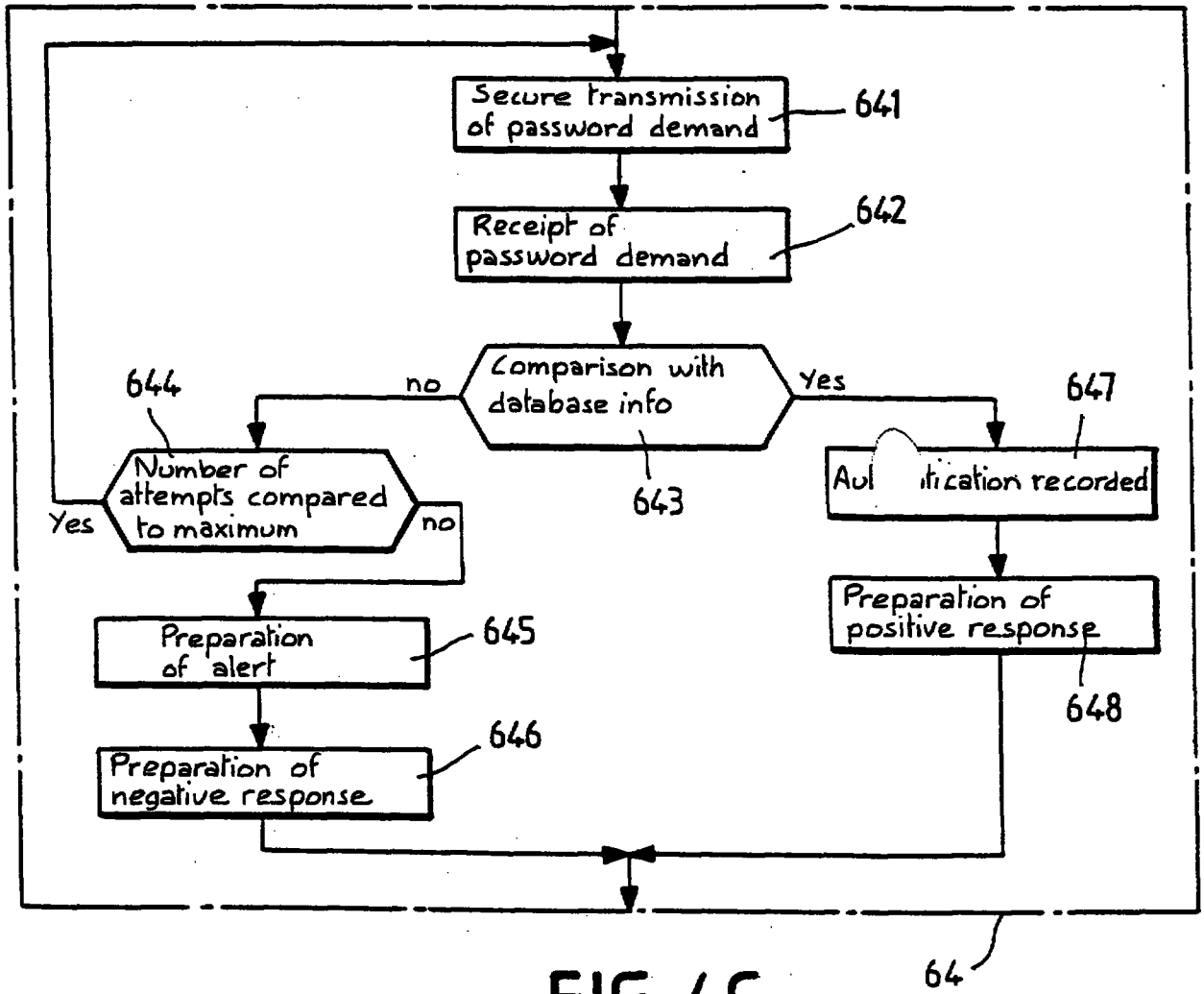

Secure transmission of password demand
641
Receipt of password demand
642
Comparison with database info
643
644
no
Yes
647
Number of attempts compared to maximum
Yes
no
Aut ification recorded
Preparation of alert
645
Preparation of negative response
646
Preparation of positive response
648
64

FIG.4C

RTMP COPY

9705507-3

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10 — A1

(11) Numéro de publication internationale: WO 96/32701

(43) Date de publication internationale: 17 octobre 1996 (17.10.96)

(21) Numéro de la demande internationale: PCT/FR96/00500

(22) Date de dépôt international: 3 avril 1996 (03.04.96)

(30) Données relatives à la priorité:
95/04533 14 avril 1995 (14.04.95) FR

(71) Déposant: G C TECH [FR/FR]; 16, place Vendôme, F-75001 Paris (FR).

(72) Inventeurs: PAYS, Paul-André; 34, rue Juliette-Adam, F-91190 Gif-sur-Yvette (FR). BEN DAHAN, Gérard; 5, rue d'Alsace, F-75010 Paris (FR).

(74) Mandataires: JOLY, Jean-Jacques etc.; Cabinet Beau-de-Loménie, 158, rue de l'Université, F-75007 Paris (FR).

(81) Etats désignés: AU, BR, CA, CN, HU, JP, KR, MX, RU, SG, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée

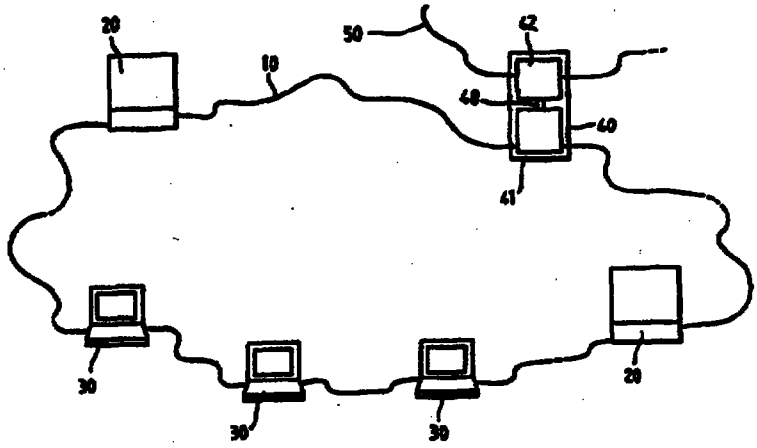
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

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

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

(57) Abstract

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 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.



(57) Abrégé

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, 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.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Arménie	GB	Royaume-Uni	MW	Malawi
AT	Autriche	GE	Géorgie	MX	Mexique
AU	Australie	GN	Guinée	NE	Niger
BB	Barbade	GR	Grèce	NL	Pays-Bas
BE	Belgique	HU	Hongrie	NO	Norvège
BF	Burkina Faso	IE	Irlande	NZ	Nouvelle-Zélande
BG	Bulgarie	IT	Italie	PL	Pologne
BJ	Bénin	JP	Japon	PT	Portugal
BR	Brésil	KE	Kenya	RO	Roumanie
BY	Bélarus	KG	Kirghizistan	RU	Fédération de Russie
CA	Canada	KP	République populaire démocratique	SD	Soudan
CF	République centrafricaine		de Corée	SE	Suède
CG	Congo	KR	République de Corée	SG	Singapour
CH	Suisse	KZ	Kazakhstan	SI	Slovénie
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovaquie
CM	Cameroun	LK	Sri Lanka	SN	Sénégal
CN	Chine	LR	Libéria	SZ	Swaziland
CS	Tchécoslovaquie	LT	Lituanie	TD	Tchad
CZ	République tchèque	LU	Luxembourg	TG	Togo
DE	Allemagne	LV	Lettonie	TJ	Tadjikistan
DK	Danemark	MC	Monaco	TT	Trinité-et-Tobago
EE	Estonie	MD	République de Moldova	UA	Ukraine
ES	Espagne	MG	Madagascar	UG	Ouganda
FI	Finlande	ML	Mali	US	Etats-Unis d'Amérique
FR	France	MN	Mongolie	UZ	Ouzbékistan
GA	Gabon	MR	Mauritanie	VN	Viet Nam