(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
4 juillet 2002 (04.07.2002)

PCT

(10) Numéro de publication internationale
WO 02/052517 A1

(51) Classification internationale des brevets[7] : G07F 19/00

(21) Numéro de la demande internationale :
PCT/FR01/04029

(22) Date de dépôt international :
18 décembre 2001 (18.12.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/17078 22 décembre 2000 (22.12.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

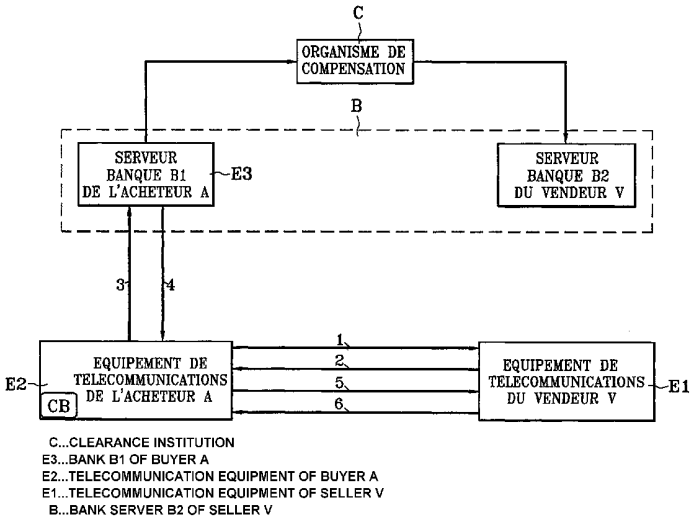
(75) Inventeurs/Déposants *(pour US seulement)* : **REMERY, Patrick** [FR/FR]; 43, rue de Cornouailles, F-14000 Caen (FR). **DESPLANQUES, Fabrice** [FR/FR]; 8, rue Ledoux, F-14000 Caen (FR). **DARBOUR, Bernard** [FR/FR]; 10, allée Baudelaire, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 14, rue Emile Dron, F-61100 Flers (FR).

(74) Mandataire : **DAUDE, Delphine**; France Telecom R & D/VAT/PI, 38-40, rue du Général Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR).

[Suite sur la page suivante]

(54) Title: PAYMENT METHOD AND SYSTEM AND TELECOMMUNICATION EQUIPMENT USED IN SAID SYSTEM

(54) Titre : PROCEDE ET SYSTEME DE PAIEMENT ET EQUIPEMENTS DE TELECOMMUNICATIONS MIS EN OEUVRE DANS CE SYSTEME



(57) **Abstract:** A buyer (A) directly transmits to his bank (B1) a message (3) containing instruction for payment of an amount (MT) for service to be delivered by a seller (V). The bank (B1) authenticates the buyer and the transaction, settles or does not settle the payment of said amount (MT), depending respectively on the positive of negative results of said authenticating operations, and sends in reply to the buyer a message (4) containing data on the acceptance or denial of said instruction. The buyer verifies the reply from his bank and sends a message (5), containing said reply to the seller, who authenticates the transaction, verifies the content of the message (5), and depending respectively on the positive or negative result of said authentication and said verification, delivers or does not deliver the service, transmitting said result to the buyer by sending a message (6).

(57) **Abrégé :** Un acheteur (A) adresse directement à sa banque (B1) un message (3) d'ordre de paiement d'un montant (MT) d'une prestation due par un vendeur (V). La banque (B1) authentifie l'acheteur et la transaction, acquitte ou non, respectivement en fonction du résultat positif ou négatif de ces authentifications, l'ordre de paiement dudit montant (MT), et envoie en réponse

[Suite sur la page suivante]

WO 02/052517 A1

(81) États désignés *(national)* **:** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

à l'acheteur un message (4) contenant des informations sur l'acceptation ou non de cet ordre. L'acheteur vérifie la réponse de sa banque et envoie un message (5), contenant cette réponse, au vendeur, lequel authentifie la transaction, vérifie le contenu du message (5), et respectivement en fonction du résultat positif ou négatif de cette authentification et de cette vérification, délivre ou non la prestation, en transmettant ce résultat à l'acheteur par l'envoie d'un message (6).

Procédé et système de paiement, et équipements de télécommunications mis en œuvre dans ce système

La présente invention concerne un procédé de paiement. Elle vise également le système de mise en œuvre de ce procédé, ainsi que des équipements de télécommunications employés dans ce système.

Plus particulièrement, l'invention concerne un procédé de paiement impliquant une première entité dite « le vendeur » disposant d'un premier équipement de télécommunications, une seconde entité dite « l'acheteur » disposant d'un second équipement de télécommunications, et une troisième entité dite "gestionnaire de comptes" regroupant d'une part la banque de l'acheteur, laquelle dispose d'un troisième équipement de télécommunications apte à établir une liaison avec le second équipement de télécommunications appartenant à l'acheteur, et, d'autre part, la banque du vendeur, ce procédé comprenant un échange préliminaire qui est établi entre le vendeur et l'acheteur par l'intermédiaire de leurs premier et second équipements respectifs et qui est destiné à l'aboutissement d'une transaction entre le vendeur et l'acheteur correspondant au paiement d'un montant d'une prestation due par le vendeur.

Un tel procédé est décrit par exemple dans le document FR 2 790 162. Plus précisément, ce procédé nécessite l'intervention d'une passerelle, telle qu'un serveur de paiement, qui a pour fonction d'authentifier l'acheteur et le vendeur et de s'assurer que le bien commandé sera effectivement payé.

Ce procédé est certes avantageux d'un point de vue confidentialité de l'achat.

Il présente toutefois l'inconvénient d'exiger de

nombreux échanges, lesquels ont pour effet de ralentir les traitements d'informations, notamment en ce qui concerne les informations échangées entre l'acheteur et sa banque, et ainsi de nuire à la rentabilité économique du système de mise en œuvre de ce procédé.

Ce procédé présente également l'inconvénient de manquer de souplesse en termes de choix dans les modalités de paiement susceptibles d'être offertes à l'acheteur, compte tenu du caractère impersonnel de la relation banque-acheteur qui est dû à l'interposition du serveur de paiement lors des échanges d'informations entre l'acheteur et sa banque.

La présente invention a notamment pour but de remédier à ces inconvénients.

A cet effet, le procédé comprend, à la suite de l'échange préliminaire entre l'acheteur et le vendeur, les échanges suivants:

a) l'acheteur adresse directement à sa banque un message d'ordre de paiement dudit montant, ce message comprenant au moins :

- des informations représentatives de l'acheteur,
- des informations représentatives du vendeur,
- ledit montant de la prestation, et
- des informations représentatives de la transaction,

b) la banque de l'acheteur authentifie l'acheteur à partir des données représentatives de l'acheteur reçues, authentifie la transaction à partir de certaines des informations représentatives de l'acheteur reçues, des

informations représentatives du vendeur reçues, des informations représentatives de la transaction reçues et dudit montant de la prestation reçu, accepte ou non, respectivement en fonction du résultat positif ou négatif de ces authentifications, l'ordre de paiement dudit montant de la prestation, et envoie en réponse à l'acheteur des informations sur l'acceptation ou non de cet ordre,

c) l'acheteur vérifie la réponse de sa banque et transmet cette réponse au vendeur avec certaines des informations représentatives de l'acheteur,

d) le vendeur authentifie la transaction au moyen desdites certaines informations représentatives de l'acheteur reçues, vérifie la réponse de la banque de l'acheteur, et respectivement en fonction du résultat positif ou négatif de cette authentification et de cette vérification, délivre ou non la prestation.

Dans des modes de réalisation préférés du procédé selon l'invention, on a recours à l'une et/ou à l'autre des dispositions suivantes :

- les informations représentatives de l'acheteur comprennent des données caractéristiques d'une modalité de paiement dudit montant de la prestation qui est choisie par l'acheteur au moment de l'échange a) ;

- les informations représentatives de la transaction comprennent des données qui sont chiffrées à l'aide d'une première clef contenue dans le second équipement de télécommunications appartenant à l'acheteur, ces données étant fonction de certaines desdites informations représentatives de l'acheteur, desdites informations représentatives du vendeur et dudit montant de la prestation, et la banque de l'acheteur authentifie cette signature lors de l'échange b) ;

- les informations sur l'acceptation ou non de l'ordre de paiement envoyées à l'acheteur lors de l'échange b) se présentent sous la forme d'un message signé par une seconde clef contenue dans ledit troisième équipement de télécommunications appartenant à la banque de l'acheteur, cette signature étant authentifiée d'une part par l'acheteur lors de l'échange c) par une troisième clef contenue dans ledit second équipement de télécommunications appartenant à l'acheteur et, d'autre part, par le vendeur lors de l'échange d), par une quatrième clef, identique à la troisième clef, contenue dans ledit premier équipement de télécommunications appartenant au vendeur ;

- la seconde clef appartenant à la banque de l'acheteur est une clef privée et les troisième et quatrième clefs appartenant respectivement à l'acheteur et au vendeur sont des clefs publiques associées à ladite seconde clef privée ;

- en cas d'annulation de ladite transaction:
lesdites étapes a), b), c) et d) de la transaction sont effectuées à l'identique, le vendeur, la banque du vendeur, et, l'acheteur, jouant respectivement le rôle de l'acheteur, de la banque de l'acheteur, et, du vendeur.

Pour ce qui est du système de mise en œuvre du procédé de paiement du genre en question,

a) le second équipement de télécommunications appartenant à l'acheteur comprend des premiers moyens de transmission aptes à adresser directement au troisième équipement de télécommunications appartenant à la banque de l'acheteur un message d'ordre de paiement dudit montant de la prestation, ledit message comprenant au moins :

- des informations représentatives de

l'acheteur,

- des informations représentatives du vendeur,
- ledit montant de la prestation, et
- des informations représentatives de la transaction,

b) le troisième équipement de télécommunications (E3) appartenant à la banque de l'acheteur comprend :

- des premiers moyens d'authentification aptes à authentifier l'acheteur à partir des informations représentatives de l'acheteur reçues, des informations représentatives du vendeur reçues, des informations représentatives de la transaction reçues et dudit montant de la prestation reçu,
- des moyens de validation aptes à accepter ou non, respectivement en fonction du résultat positif ou négatif de ces authentifications, l'ordre de paiement dudit montant de la prestation,
- et des seconds moyens de transmission aptes à envoyer au second équipement de télécommunications appartenant à l'acheteur des informations sur l'acceptation ou non de cet ordre,

c) le second équipement de télécommunications de l'acheteur comprenant en outre des premiers moyens de vérification aptes à vérifier la réponse de la banque de l'acheteur, laquelle réponse est envoyée au premier équipement de télécommunications du vendeur avec certaines

des données représentatives de l'acheteur par lesdits premiers moyens de transmission,

d) le premier équipement de télécommunications appartenant au vendeur comprend :

- des seconds moyens d'authentification de la transaction au moyen desdites certaines informations représentatives de l'acheteur reçues,
- et des seconds moyens de vérification de la réponse du troisième équipement de télécommunications appartenant à la banque de l'acheteur.

Pour ce qui est des équipements de télécommunications utilisés dans le système selon l'invention :

- les premier et second équipements de télécommunications consistent chacun en un terminal connectable au réseau téléphonique ;
- et le troisième équipement de télécommunications consiste en un serveur.

D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description suivante d'une de ses formes de réalisation, donnée à titre d'exemple non limitatif, en regard de la figure unique jointe.

Cette figure illustre l'architecture générale du système de paiement de l'invention et les différents échanges établis entre les divers équipements de télécommunications.

Sur la figure annexée, la référence numérique E1 désigne un premier équipement de télécommunications appartenant à un vendeur V, la référence numérique E2 un

second équipement de télécommunications appartenant à un acheteur A, la référence numérique E3 un troisième équipement de télécommunications appartenant à une banque B1 de l'acheteur A, et la référence numérique B2 une banque du vendeur V.

Dans l'exemple représenté, les banques B1 et B2 sont regroupées au sein d'une même entité appelée « gestionnaire de comptes » B.

L'opération de paiement qui concerne plus spécialement l'invention est précédée d'un échange préliminaire entre le vendeur V et l'acheteur A, cet échange étant symbolisé par les flèches 1 et 2 sur la figure. Lors de cet échange, l'acheteur A envoie un message 1 de commande de bien au vendeur V, et le vendeur V communique en réponse à l'acheteur A un message 2 indiquant le montant MT correspondant à la prestation due, ainsi que l'offre d'achat.

Un tel échange peut se faire selon de multiples modalités qui dépendent de l'équipement de télécommunications de l'acheteur A et du vendeur V.

Dans l'exemple représenté, le premier équipement de télécommunications E1 du vendeur V et le second équipement de télécommunications E2 de l'acheteur A consistent chacun en un terminal connectable à un réseau téléphonique.

D'une manière avantageuse, les premier et second équipements de télécommunications peuvent consister indépendamment l'un de l'autre en, par exemple, un téléphone mobile du type GSM, un Minitel (marque déposée), ou un ordinateur personnel PC connecté au réseau Internet.

Ainsi, l'échange préliminaire entre le vendeur V et l'acheteur A, de même que les échanges ultérieurs, peuvent être effectués par exemple :

- entre le téléphone mobile de l'acheteur A et le terminal du vendeur V,

- entre le téléphone mobile de l'acheteur A et le téléphone mobile du vendeur V, par exemple par échange de messages courts (« short messages »),

- à partir uniquement du téléphone mobile de l'acheteur A, ce téléphone étant muni à cet effet de deux interfaces qui sont destinées à recevoir respectivement les modules sécurisés de l'acheteur A et du vendeur V, tels que par exemple une carte bancaire à puce (CB) ou une carte porte-monnaie électronique (PME), un telle possibilité autorisant avantageusement le paiement de proximité,

- ou encore à partir du seul téléphone mobile de l'acheteur A, les informations reçues en provenance du vendeur V étant alors saisies sur le clavier du téléphone mobile de l'acheteur A.

Dans l'exemple représenté, le premier équipement de télécommunications E1 appartenant au vendeur V est un terminal connectable à un réseau téléphonique, tandis que le second équipement de télécommunications E2 appartenant à l'acheteur A est un téléphone mobile du type GSM apte à recevoir le module sécurisé de l'acheteur A.

Lors de l'échange préliminaire entre le vendeur V et l'acheteur A, l'acheteur A envoie au vendeur V un message 1 de commande de bien, via son téléphone mobile E1.

Le vendeur V transmet alors en réponse à l'acheteur A, via son terminal E1, un message 2 définissant le montant MT de la prestation due, ainsi que l'offre d'achat. Plus précisément, ce message comprend essentiellement :

- des informations non confidentielles représentatives du vendeur V, telles que l'identifiant du compte du vendeur V, la date et l'heure de la transaction,

un numéro chronologique des transactions effectuées par le vendeur V,

- et des informations confidentielles représentatives du vendeur V qui sont les informations ci-dessus et l'offre commerciale regroupées de façon confidentielle, par exemple au moyen d'un algorithme de condensation connu en tant que tel, ce condensé, désigné par la référence CV, ayant pour but de maintenir confidentielle l'offre commerciale proposée à l'acheteur, en particulier vis à vis de la banque de l'acheteur.

Afin d'obtenir une sécurité accrue de l'achat, les informations confidentielles représentatives du vendeur V peuvent en outre être représentées sous la forme d'un message signé sign(CV) à l'aide d'une clef secrète (algorithme symétrique), ou, privée (algorithme à clé publique), calculée dans le terminal E1 du vendeur V, de manière à garantir le contenu de l'offre commerciale.

L'acheteur A introduit alors son module sécurisé, par exemple, sa carte bancaire à puce CB, dans son téléphone mobile E2 et tape son code confidentiel CC de façon à être authentifié par ledit module.

Si le résultat de cette authentification s'avère positif, le module sécurisé CB de l'acheteur A :

- authentifie le vendeur V et l'offre d'achat associée, par vérification de la signature sign(CV), uniquement dans le cas où le message sign(CV) a été envoyé à l'acheteur A,

- vérifie le condensé CV des informations confidentielles reçues, par calcul de CV, puis par vérification du condensé calculé CV avec le condensé CV reçu,

- calcule un condensé CA des informations

confidentielles représentatives de l'acheteur A, lesquelles comprennent essentiellement l'identifiant du compte de l'acheteur A, la date et l'heure de la transaction, un numéro chronologique des transactions effectuées par l'acheteur A, le condensé CA ayant pour but de maintenir confidentielles les informations bancaires de l'acheteur en particulier vis à vis du vendeur,

- calcule un condensé CT de la transaction en fonction desdits condensés CA, CV et de certaines des informations non confidentielles représentatives du vendeur V,

- et calcule la signature ST des informations représentatives de la transaction, à savoir le condensé CT et le montant MT de la prestation, lesquelles sont signées par une première clef secrète, ou privée contenue dans la carte à puce CB.

De manière avantageuse, les informations confidentielles représentatives de l'acheteur A comportent en outre le choix d'une modalité de paiement MP qui s'offre à l'acheteur A, à savoir paiement à crédit, paiement à débit différé, paiement à débit immédiat ou autres. De telles modalités se présentent par exemple sous la forme d'options contenues dans un même menu qui s'affiche sur l'écran du téléphone mobile E2, et que sélectionne l'acheteur A.

Si le résultat de la vérification du condensé CV des informations confidentielles représentatives du vendeur V s'avère positif, l'échange a) suivant a lieu.

La carte SIM (« Subscriber Identification Module ») du téléphone mobile E2 de l'acheteur A adresse directement au troisième équipement de télécommunications E3 de la banque B1 de l'acheteur A, lequel équipement est un serveur, un message 3 d'ordre de paiement du montant MT de la

prestation, ce message comprenant :

- des informations non confidentielles vis à vis de la banque représentatives de l'acheteur A, telles que l'identifiant du compte de l'acheteur A, la date et l'heure de la transaction, un numéro chronologique des transactions effectuées par l'acheteur A,

- le condensé CA des informations représentatives de l'acheteur A,

- la modalité de paiement MP décidée par l'acheteur A,

- les informations non confidentielles, vis à vis de la banque, représentatives du vendeur V,

- le condensé CV des informations confidentielles, vis à vis de la banque, représentatives du vendeur V,

- le montant MT de la prestation, et

- des informations représentatives de la transaction, telles que le condensé CT et ST.

Il convient de noter que le message d'ordre de paiement ne contient aucune donnée relative à l'offre d'achat, la confidentialité de la nature du bien commandé par l'acheteur A étant ainsi parfaitement assurée.

Par ailleurs, le fait que ce message d'ordre de paiement 3 soit adressé directement par l'acheteur A à sa banque B1 permet ainsi de réduire le plus possible une répudiation de l'ordre par l'acheteur.

A partir de la réception du message 3 envoyé par l'acheteur A, l'échange b) suivant a lieu.

Le serveur E3 de la banque B1 de l'acheteur A :

- authentifie l'acheteur A par calcul du condensé CA dans un module de calcul, puis par vérification dudit condensé calculé CA avec le condensé CA reçu dans un module de comparaison,

- authentifie la transaction :
  - par calcul du condensé CT à partir du condensé CA reçu, du condensé CV reçu, des informations non confidentielles représentatives du vendeur V reçues, puis par vérification du condensé CT calculé avec le condensé CT reçu,
  - par calcul de la signature ST à partir du condensé CT reçu et du montant MT reçu, puis par vérification de ladite signature calculée ST avec la signature ST reçue.

Respectivement en fonction du résultat positif ou négatif de ces authentifications et l'état du compte bancaire de l'acheteur A, la banque B1 de l'acheteur A accepte ou non l'ordre de paiement dudit montant MT de la prestation. Pour ce faire, le serveur E3 de la banque B1 de l'acheteur A envoie vers la carte SIM du téléphone mobile E2 de l'acheteur A un message 4 qui contient des informations sur l'acceptation ou non de l'ordre, lesquelles regroupent le condensé CT de la transaction, le montant MT de la transaction, le numéro chronologique des transactions effectuées par le vendeur V, ainsi qu'une donnée « statut de la transaction », SW. Cette donnée SW, peut correspondre à l'un des états suivants :

- transaction acceptée avec crédit,
- transaction acceptée avec débit différé,
- transaction acceptée avec débit immédiat,
- transaction refusée.

Les informations sur l'acceptation ou non de l'ordre de paiement peuvent être enregistrées dans la carte à puce de l'acheteur A et/ou le terminal du vendeur, et être

effacées par la suite lorsque l'acheteur A et/ou le vendeur V considère cet ordre comme obsolète.

Par ailleurs, le message 4 est avantageusement signé à l'aide d'une seconde clef, de préférence privée, contenue dans le serveur E3 de la banque B1. Ceci permet ainsi de garantir l'authenticité de la transaction.

Dans le cas où la donnée SW ne correspond pas à l'état « transaction refusée », le paiement du montant MT de la prestation est effectué automatiquement par la banque B1 de l'acheteur A au profit de la banque B2 du vendeur V, par l'intermédiaire d'un organisme de compensation C connu en soi, tel que le service interbancaire de télécompensation.

A partir de la réception du message 4, l'échange c) a lieu. La carte à puce CB de l'acheteur A authentifie la signature AT au moyen d'une troisième clef contenue dans la carte à puce CB, laquelle est une clef publique associée à la clef privée contenue dans le serveur E3 de la banque B1, puis vérifie la donnée SW. Une fois effectuées ces opérations, la carte SIM du téléphone mobile de l'acheteur A envoie un message 5 au terminal E1 du vendeur V, ce message comprenant :

- le condensé CA,
- la signature AT de l'acceptation ou non de la transaction,
- ainsi que la donnée SW.

Suite à la réception du message 5, l'échange d) a lieu. Le terminal E1 du vendeur V authentifie la transaction par calcul du condensé CT à partir du condensé CA reçu et du condensé CV calculé lors de l'envoi du message 2 en début de transaction. Puis le terminal E1 du vendeur V :

- authentifie la signature AT au moyen d'une quatrième clef, laquelle est identique à la troisième clef

contenue dans la carte à puce CB du téléphone mobile E2 de l'acheteur A,

- et vérifie la donnée SW.

Si le résultat de ces opérations s'avère positif et que la donnée SW ne correspond pas à l'état « transaction refusée », le vendeur V délivre en toute confiance la prestation. Il envoie alors à l'acheteur A un message 6 de confirmation de la délivrance de la prestation.

Dans le cas où une telle transaction vient à être annulée, une nouvelle transaction, identique à celle qui est décrite ci-dessus, est établie. Mais dans ce cas, le vendeur V joue le rôle de l'acheteur A, et l'acheteur A, celui du vendeur V.

Le système de paiement qui vient d'être décrit ci-dessus présente les avantages suivants :

- une grande facilité d'utilisation de ce système par l'acheteur A, laquelle peut être liée à l'emploi du téléphone mobile, dont l'intérêt est d'être doté de fonctions d'envoi ou de réception de données ainsi que d'une interface pouvant loger un module sécurisé,

- une plus grande possibilité de fidélisation de l'acheteur A auprès de sa banque B1, compte tenu du fait qu'ils ne sont plus séparés par une passerelle,

- la suppression d'une liste noire chez le vendeur V,

- la suppression des connexions du vendeur V auprès de sa banque B2 visant à la transmission de son chiffre d'affaires quotidien,

- et la suppression des commissions dues par le vendeur V à sa banque B2.

REVENDICATIONS

1.Procédé de paiement impliquant une première entité dite « le vendeur (V) » disposant d'un premier équipement de télécommunications (E1), une seconde entité dite « l'acheteur (A) » disposant d'un second équipement de télécommunications (E2), et une troisième entité dite "gestionnaire de comptes" (B) regroupant d'une part la banque (B1) de l'acheteur (A), laquelle dispose d'un troisième équipement de télécommunications (E3) apte à établir une liaison avec le second équipement de télécommunications (E2) appartenant à l'acheteur (A), et, d'autre part, la banque (B2) du vendeur (V), ce procédé comprenant un échange préliminaire qui est établi entre le vendeur (V) et l'acheteur (A) par l'intermédiaire de leurs premier et second équipements respectifs et qui est destiné à l'aboutissement d'une transaction entre le vendeur (V) et l'acheteur (A) correspondant au paiement d'un montant (MT) d'une prestation due par le vendeur (V),

caractérisé en ce que :

à la suite de cet échange préliminaire, le procédé comprend les échanges suivants:

a) l'acheteur (A) adresse directement à sa banque (B1) un message d'ordre de paiement dudit montant (MT), ce message comprenant au moins :

- des informations représentatives de l'acheteur (A),
- des informations représentatives du vendeur (V),
- ledit montant(MT) de la prestation, et
- des informations (CT, ST) représentatives

de la transaction,

b)la banque (B1) de l'acheteur (A) authentifie l'acheteur (A) à partir des données représentatives de l'acheteur reçues, authentifie la transaction à partir de certaines des informations représentatives de l'acheteur (A) reçues, des informations représentatives du vendeur (V) reçues, des informations représentatives de la transaction reçues et dudit montant (MT) de la prestation reçu, accepte ou non, respectivement en fonction du résultat positif ou négatif de ces authentifications, l'ordre de paiement dudit montant (MT) de la prestation, et envoie en réponse à l'acheteur (A) des informations sur l'acceptation ou non de cet ordre,

c)l'acheteur (A) vérifie la réponse de sa banque (B1) et transmet cette réponse au vendeur (V) avec certaines des informations représentatives de l'acheteur (A),

d)le vendeur (V) authentifie la transaction au moyen desdites certaines informations représentatives de l'acheteur (A) reçues, vérifie la réponse de la banque (B1) de l'acheteur (A), et respectivement en fonction du résultat positif ou négatif de cette authentification et de cette vérification, délivre ou non la prestation.

2. Procédé selon la revendication 1, dans lequel les informations représentatives de l'acheteur (A) comprennent des données (MP) caractéristiques d'une modalité de paiement dudit montant (MT) de la prestation qui est choisie par l'acheteur (A) au moment de l'échange a).

3. Procédé selon la revendication 1 ou 2, dans lequel les informations (CT, ST) représentatives de la transaction comprennent des données qui sont chiffrées à l'aide d'une première clef contenue dans le second équipement de télécommunications (E2) appartenant à

l'acheteur (A), ces données étant fonctions de certaines desdites informations représentatives de l'acheteur (A), desdites informations représentatives du vendeur (V) et dudit montant (MT) de la prestation, et la banque (B1) de l'acheteur (A) authentifie cette signature lors de l'échange b).

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel les informations sur l'acceptation ou non de l'ordre de paiement envoyées à l'acheteur (A) lors de l'échange b) se présentent sous la forme d'un message signé (AT) par une seconde clef contenue dans ledit troisième équipement de télécommunications (E3) appartenant à la banque (B1) de l'acheteur (A), cette signature (AT) étant authentifiée d'une part par l'acheteur (A) lors de l'échange c) par une troisième clef contenue dans ledit second équipement de télécommunications (E2) appartenant à l'acheteur (A) et, d'autre part, par le vendeur (V) lors de l'échange d) par une quatrième clef, identique à la troisième clef, contenue dans ledit premier équipement de télécommunications (E1) appartenant au vendeur (V).

5. Procédé selon la revendication 4, dans lequel la seconde clef appartenant à la banque (B1) de l'acheteur (A) est une clef privée et les troisième et quatrième clefs appartenant respectivement à l'acheteur (A) et au vendeur (V) sont des clefs publiques associées à ladite seconde clef privée.

6. Procédé d'annulation d'une transaction effectuée par le procédé selon l'une quelconque des revendications 1 à 5, dans lequel lesdites étapes a), b), c) et d) de la transaction sont effectuées à l'identique, le vendeur (V), la banque (B2) du vendeur, et, l'acheteur (A), jouant respectivement le rôle de l'acheteur (A), de la banque (B1)

de l'acheteur, et, du vendeur (V).

7. Système de paiement pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 6, comprenant un premier équipement de télécommunications (E1) utilisé par un vendeur (V), un second équipement de télécommunications (E2) utilisé par un acheteur (A), un troisième équipement de télécommunications (E3) utilisé par la banque (B1) de l'acheteur (A) et apte à établir une liaison avec le second équipement de télécommunications (E2) de l'acheteur (A),

caractérisé en ce que :

a) le second équipement de télécommunications (E2) appartenant à l'acheteur (A) comprend des premiers moyens de transmission aptes à adresser directement au troisième équipement de télécommunications (E3) appartenant à la banque (B1) de l'acheteur (A) un message d'ordre de paiement dudit montant (MT) de la prestation, ledit message comprenant au moins :

- des informations représentatives de l'acheteur (A),
- des informations représentatives du vendeur (V),
- ledit montant (MT) de la prestation, et
- des informations (CT, ST) représentatives de la transaction,

b) le troisième équipement de télécommunications (E3) appartenant à la banque (B1) de l'acheteur (A) comprend :

- des premiers moyens d'authentification aptes à authentifier l'acheteur (A) à partir des informations représentatives de l'acheteur (A) reçues, des informations représentatives du vendeur (V) reçues, des informations

représentatives de la transaction reçues et dudit montant (MT) de la prestation reçu,

- des moyens de validation aptes à accepter ou non, respectivement en fonction du résultat positif ou négatif de ces authentifications, l'ordre de paiement dudit montant (MT) de la prestation,

- et des seconds moyens de transmission aptes à envoyer au second équipement de télécommunications (E2) appartenant à l'acheteur (A) des informations sur l'acceptation ou non de cet ordre,

c)le second équipement de télécommunications (E2) de l'acheteur (A) comprenant en outre des premiers moyens de vérification aptes à vérifier la réponse de la banque (B1) de l'acheteur (A), laquelle réponse est envoyée au premier équipement de télécommunications (E1) du vendeur (V) avec certaines des données représentatives de l'acheteur (A) par lesdits premiers moyens de transmission,

d)le premier équipement de télécommunications (E1) appartenant au vendeur (V) comprend :

- des seconds moyens d'authentification de la transaction au moyen desdites certaines informations représentatives de l'acheteur (A) reçues,

- et des seconds moyens de vérification de la réponse du troisième équipement de télécommunications (E3) appartenant à la banque (B1) de l'acheteur (A).

8. Equipement de télécommunications utilisé par un acheteur (A) dans le système selon la revendication 7, caractérisé en ce qu'il consiste en un terminal connectable

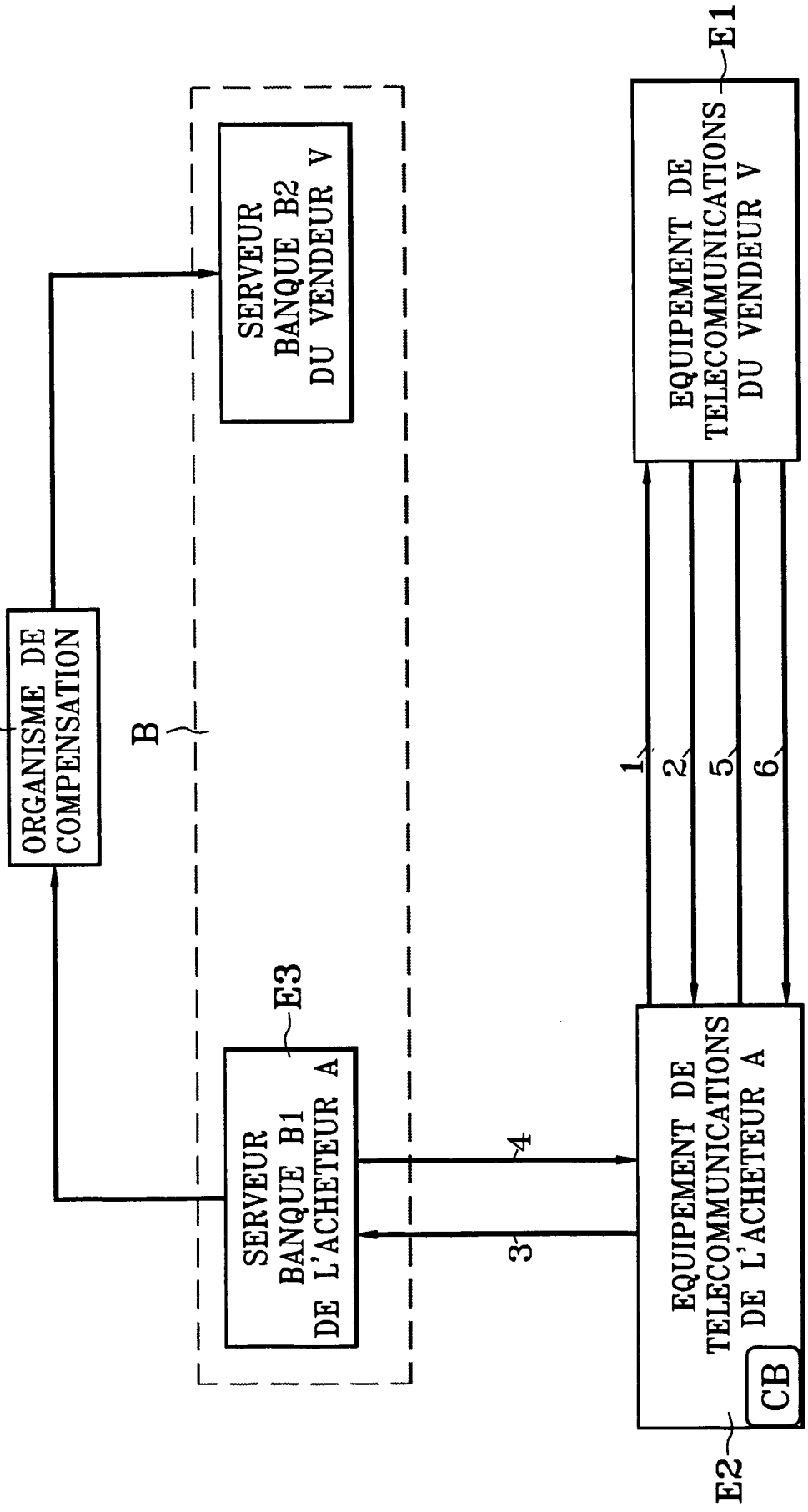
au réseau téléphonique.

9. Equipement de télécommunications selon la revendication 8, dans lequel le terminal est un téléphone mobile de type GSM.

10. Equipement de télécommunications utilisé par un vendeur (V) dans le système selon la revendication 7, caractérisé en ce qu'il consiste en un terminal connectable au réseau téléphonique.

11. Equipement de télécommunications utilisé par l'une quelconque des banques (B1, B2) dans le système selon la revendication 7, caractérisé en ce qu'il consiste en un serveur.

FIG. 1


C
ORGANISME DE COMPENSATION
B
SERVEUR BANQUE B2 DU VENDEUR V
E3
SERVEUR BANQUE B1 DE L'ACHETEUR A
E1
EQUIPEMENT DE TELECOMMUNICATIONS DU VENDEUR V
1
2
3
4
5
6
EQUIPEMENT DE TELECOMMUNICATIONS DE L'ACHETEUR A
CB
E2

INTERNATIONAL SEARCH REPORT

tional Application No
PCT/FR 01/04029

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 17833 A (PRANGE STEFAN ;LAHR ANDREAS (DE); SIEMENS AG (DE)) 30 March 2000 (2000-03-30) page 7, line 11 -page 9, line 28 figure 1 ---	1-5,7-11
X	US 6 029 150 A (KRAVITZ DAVID WILLIAM) 22 February 2000 (2000-02-22) figures 1,2 column 11, line 48 -column 13, line 48	1,2,8,11
A	-----	3-7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 May 2002	16/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Papastefanou, E

INTERNATIONAL SEARCH REPORT

Ir...tional Application No
PCT/FR 01/04029

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0017833 A	30-03-2000	DE 19843439 A1	30-03-2000
		CN 1319219 T	24-10-2001
		WO 0017833 A1	30-03-2000
		EP 1116194 A1	18-07-2001
US 6029150 A	22-02-2000	AU 4588197 A	24-04-1998
		EP 0944882 A1	29-09-1999
		WO 9814921 A1	09-04-1998

RAPPORT DE RECHERCHE INTERNATIONALE

De le internationale No
PCT/FR 01/04029

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 00 17833 A (PRANGE STEFAN ;LAHR ANDREAS (DE); SIEMENS AG (DE)) 30 mars 2000 (2000-03-30) page 7, ligne 11 -page 9, ligne 28 figure 1	1-5,7-11
X	US 6 029 150 A (KRAVITZ DAVID WILLIAM) 22 février 2000 (2000-02-22) figures 1,2 colonne 11, ligne 48 -colonne 13, ligne 48	1,2,8,11
A		3-7

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 mai 2002	16/05/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Papastefanou, E

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 01/04029

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0017833 A	30-03-2000	DE 19843439 A1	30-03-2000
		CN 1319219 T	24-10-2001
		WO 0017833 A1	30-03-2000
		EP 1116194 A1	18-07-2001
US 6029150 A	22-02-2000	AU 4588197 A	24-04-1998
		EP 0944882 A1	29-09-1999
		WO 9814921 A1	09-04-1998