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 7 : G07F 7/10, H04Q 7/32

A1

(11) Numéro de publication internationale: WO 00/49585

(43) Date de publication internationale: 24 août 2000 (24.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00412

(22) Date de dépôt international: 18 février 2000 (18.02.00)

(30) Données relatives à la priorité:
99/02093 19 février 1999 (19.02.99) FR

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

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean–Claude [FR/FR]; 4, rue des Loisirs, F–14610 Epron (FR). LEVIONNAIS, Philippe [FR/FR]; 23, rue du Clos Beaumois, F–14000 Caen (FR).

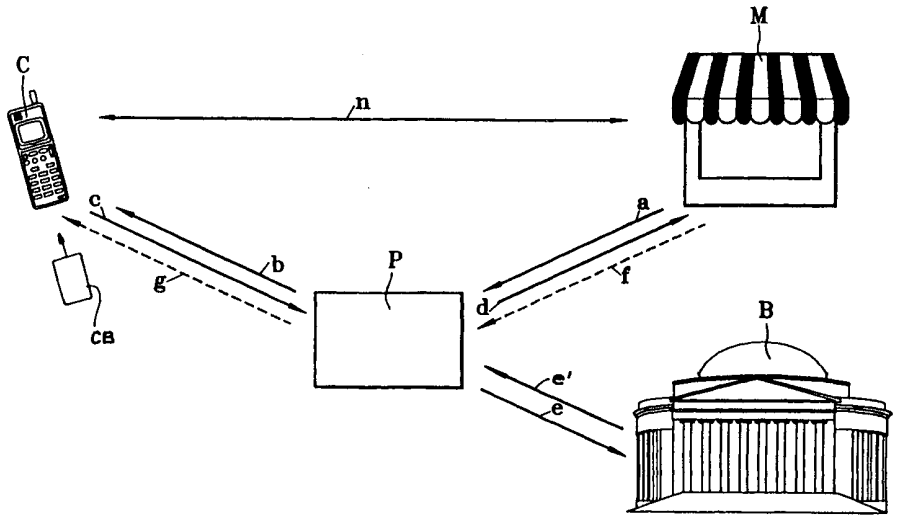
(74) Mandataire: DU BOISBAUDRY, Dominique; Société de Protection des Inventions, 3, rue du Docteur Lancereaux, F–75008 Paris (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, 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), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: TELEPAYMENT METHOD AND SYSTEM FOR IMPLEMENTING SAID METHOD

(54) Titre: PROCEDE DE TELEPAIEMENT ET SYSTEME POUR LA MISE EN OEUVRE DE CE PROCEDE



(57) Abstract

The invention concerns a method wherein the client's equipment is a mobile equipment, for example of the GSM–type. Besides the client (C) and the trader (M), a gateway (P) intervenes in the transaction, to authenticate the client and the trader and ensure that the good ordered will actually be paid for. The client's equipment can operate with a bank payment card.

(57) Abrégé

L'équipement du client est un équipement mobile, par exemple de type GSM. En plus du client (C) et du commerçant (M), une passerelle (P) intervient dans la transaction, authentifie le client et le commerçant et s'assure que le bien commandé sera bien payé. L'équipement du client peut travailler avec une carte de paiement bancaire.

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.

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

PROCEDE DE TELEPAIEMENT ET SYSTEME POUR LA MISE EN OEUVRE DE CE PROCEDE

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé de télépaiement et un système pour la mise en oeuvre de ce procédé.

Etat de la technique antérieure

Le télépaiement, ou paiement à distance, est bien connu. Il peut prendre des formes plus ou moins élaborées :

- par téléphone, un client peut communiquer son numéro de carte bancaire à un commerçant,
- avec un ordinateur personnel, le client peut transmettre ce numéro au serveur du commerçant,
- avec les appareils de type Minitel (marque déposée), qui disposent d'un lecteur de carte à puce, l'utilisateur insère sa carte bancaire dans le lecteur et fournit un code confidentiel ; si le code est correct, le numéro de la carte est transmis au commerçant.

Ces procédures n'offrent pas toujours la sécurité souhaitée. A cet égard, le télépaiement soulève des difficultés spécifiques. Ainsi, la protection de ce qu'on appelle les "identifiants" des cartes bancaires (numéro de carte/date de validité, etc...) appelés aussi PAN ("Primary Account Number"), doit être assurée efficacement ; l'espionnage sur le réseau ou la réutilisation de ces numéros par un commerçant

indélicat, sont des risques sérieux qu'il faut prendre en compte dans le paiement à distance.

Par ailleurs, le caractère impersonnel de la relation client-commerçant peut inquiéter le client qui se pose inévitablement la question de savoir si le commerçant est sérieux et s'il va livrer effectivement le bien commandé. L'authentification du commerçant est donc nécessaire.

Réciproquement, se pose le problème du refus possible de la marchandise par le client : pour que le client n'ait pas les moyens de nier son achat, il faut un mécanisme fort de signature électronique reconnu qui permette de l'engager réglementairement dans sa décision d'achat. Si de tels mécanismes ne sont pas mis en place, il existe alors, pour le commerçant honnête, un risque réel de non paiement.

Toutes ces difficultés sont des freins au développement du commerce électronique. La présente invention a justement pour but de remédier à ces difficultés.

Exposé de l'invention

A cette fin, l'invention propose d'abord d'utiliser, au niveau du client, des équipements particuliers qui sont des équipements mobiles, par exemple du type GSM ("Global System for Mobile Communications"). Elle propose aussi l'intervention d'une entité qui va s'assurer du bon déroulement de la transaction. A propos du premier aspect de l'invention, on sait que les équipements mobiles se développent rapidement en France et à l'étranger : 10 millions d'équipements en France fin 98, et dans le monde, 100 millions. Il faut rappeler les fonctions que l'on

trouve dans un mobile, en particulier de type GSM, afin de mieux comprendre l'intérêt du procédé de télépaiement selon l'invention.

Dans les téléphones GSM, on retrouve les fonctions classiques d'un téléphone fixe (numéroter pour appeler, être appelé, communiquer en vocal) et des fonctions d'envoi ou de réception de données :

1. envoi de données en DTMF ("Dual Tone Multi Frequency") pendant la communication vocale, données correspondant au code des touches que l'utilisateur actionne ;
2. émission-réception de messages courts de texte ("short messages" ou SM), qui peuvent être mémorisés dans une carte dite carte d'identification d'abonné ou carte SIM ("Subscriber Identification Module") ; ces messages peuvent être affichés sur un écran de l'équipement mobile grâce à des touches particulières ; ces messages restent dans la carte jusqu'à ce que l'utilisateur les efface ;
3. émission-réception de messages courts (SM) de données, fabriqués et traités par un programme dit "toolkit", TK en abrégé ;
4. les programmes auxquels il est fait allusion ci-dessus sont des programmes qui résident dans la carte SIM et qui permettent, en plus des traitements internes (calcul, gestion de données) que peut faire tout programme, d'agir sur l'affichage du mobile, de saisir les touches du clavier actionnées par l'utilisateur, de recevoir un message SM, d'émettre un message SM ;

5. une possibilité nouvelle est apparue sur certains équipements mobiles : admettre une deuxième carte à puce, en plus de la carte SIM, ce qui permet, par exemple, d'utiliser un portable GSM avec une carte de paiement bancaire (CB) comme il en existe près de 30 millions en France, ou une carte porte-monnaie électronique (PME) comme il en existe beaucoup en Europe ou dans le monde.

On peut noter que les équipements mobiles anciens (première génération, c'est-à-dire les GSM en phases 1 et 2) possédaient seulement les fonctions N°1 et 2. Les fonctions N°3 et 4 sont apparues récemment et s'étendront rapidement à tous les mobiles dits de deuxième génération (phase 2+) ; la possibilité N°5 ne concerne pour l'instant qu'un faible pourcentage des mobiles de deuxième génération mais est appelée à se développer.

Selon le second aspect de l'invention, le télépaiement s'effectue par l'entremise d'une entité qu'on appellera "passerelle", faisant office de serveur de paiement. Cette passerelle possède un équipement de télécommunications lui permettant d'établir, avec un commerçant, une liaison quelconque (téléphonique, par le réseau Internet, etc...) et avec le client une liaison téléphonique utilisant l'équipement mobile GSM de celui-ci. La passerelle a essentiellement pour fonction d'établir une liaison entre le commerçant et le client en authentifiant à la fois le commerçant et le client, et de recevoir les données confidentielles du client lui permettant d'effectuer le paiement.

La sécurité du client et du commerçant est ainsi assurée et le paiement effectué.

De façon plus précise, la présente invention a pour objet un procédé de télépaiement impliquant une première entité dite "le client" disposant d'un premier équipement téléphonique et une deuxième entité dite "le commerçant" disposant d'un deuxième équipement de télécommunications, ce procédé étant caractérisé en ce que l'équipement du client est un équipement téléphonique mobile et en ce qu'il implique en outre une troisième entité, dite "passerelle" disposant d'un troisième équipement de télécommunications apte à établir une liaison avec l'équipement du commerçant et une liaison téléphonique avec l'équipement du client, ce procédé comprenant les échanges suivants entre les équipements des trois entités :

a) le commerçant adresse à la passerelle des données définissant une offre de prestation, avec notamment le montant à acquitter par le client, et ajoute à ces données des données d'identification du commerçant,

b) la passerelle authentifie le commerçant, convertit les données de l'offre en un message adapté aux performances de l'équipement mobile du client et adresse au client ce message ainsi que des données d'authentification de la passerelle,

c) le client authentifie la passerelle et adresse en retour à celle-ci un message d'accord, ainsi que des informations confidentielles permettant le paiement du montant de la prestation,

d) la passerelle authentifie le client, vérifie que le paiement est possible et adresse au commerçant un message stipulant que le montant de la prestation est bien susceptible d'être acquitté.

De préférence, l'équipement mobile du client est de type GSM, quelle que soit la génération (connue ou à venir).

La troisième entité peut, dans certains cas, être située chez le commerçant, ou dans d'autres cas, dans la banque.

La présente invention a également pour objet un système pour la mise en oeuvre de ce procédé.

Brève description du dessin

La figure unique annexée illustre l'architecture générale du système de l'invention et les différents échanges établis entre les divers équipements.

Exposé de modes particuliers de réalisation

Sur la figure annexée, C désigne l'équipement mobile du client, M l'équipement du commerçant, P l'équipement de la passerelle, B une ou des banques et CB une carte de paiement bancaire ou une carte PME. Les flèches symbolisent des échanges entre tous ces équipements. On supposera, dans la description qui suit, que l'équipement mobile du client est un équipement GSM et que la carte est une carte bancaire. Pour plus de clarté, la passerelle est dissociée des équipements du commerçant et de la banque, mais, dans certains cas, cette passerelle pourrait être située chez le commerçant (ou dans la banque).

L'opération de télépaiement qui concerne plus spécialement l'invention peut être précédée d'une négociation entre le client et le commerçant, négociation symbolisée par la double flèche n sur la figure. Le commerçant peut être une personne physique munie d'un téléphone ou un serveur vocal. Dans ce cas, la négociation n consiste en un échange de messages vocaux envoyés par le serveur au client et de réponses du client sous forme de codes DTMF correspondant aux touches actionnées sur le clavier de l'équipement du mobile. Par ailleurs, le client doit donner au commerçant son numéro de mobile, à moins que ce commerçant ait un téléphone indiquant le numéro de téléphone appelant.

Après cet échange préliminaire, le client raccroche et la phase de négociation est terminée. On peut observer aussi que le commerçant peut être également un serveur sur Internet. Suivent alors des échanges permettant un engagement réciproque du client et du marchand sur l'offre et le paiement. Le commerçant adresse un message a) à la passerelle P par exemple par un Minitel (marque déposée) ou par un équipement connecté au réseau Internet, communique à la passerelle P une description contractuelle de la prestation proposée et son prix. Par exemple, ce message contiendra : le numéro du mobile, la date, l'identification du commerçant, l'identification du bien, la description du bien, la quantité, le prix, ... En outre, le message a) contient des données de sécurité permettant à la passerelle P d'authentifier le commerçant M.

Un message b) est alors envoyé au client C sous une forme dépendant du type d'équipement de mobile GSM et de ses capacités.

Par un message c), le client C accepte ou refuse l'offre qui lui est faite. En cas d'acceptation, la passerelle P peut demander une autorisation à la banque B par un échange e). Celle-ci peut adresser une réponse e' à la passerelle. Dans le cas où le paiement est accepté, la passerelle P adresse par un message d) au commerçant M. Eventuellement, le commerçant M peut envoyer une confirmation f) à la passerelle P, pour indiquer, par exemple, une date de livraison, ou bien une information particulière telle qu'un code d'accès à un hôtel où une chambre aura été réservée. Cette confirmation est adressée au client par le message g). Dans un autre exemple, le client obtient d'un prestataire quelconque (Télévision, Cinéma, Internet) un code d'accès qui lui permet d'accéder effectivement à un service : ce code peut être, par exemple, tapé sur la télécommande du décodeur de télévision pour voir effectivement le programme précédemment acheté, ou encore tapé sur le clavier d'un portillon donnant accès au cinéma, ou sur le clavier de l'ordinateur personnel au moment de se connecter à ce service. Cette confirmation est répercutée sous forme de message court (SM) envoyé au client.

On peut observer que, dans le contexte de la téléphonie mobile, un certain temps peut séparer chacune de ces différentes phases : en effet, après la négociation préliminaire, les conditions de propagation liées au déplacement du mobile ou à l'état de sa batterie font peut être que le message a) sera retardé de plusieurs minutes. Il faut donc que le système soit

organisé pour prendre en compte tous ces aspects spécifiques de la technologie GSM.

Pour décrire plus avant la nature des échanges, on peut distinguer quatre cas selon la nature de l'équipement mobile du client :

1. Cas d'un équipement mobile de première génération

Dans ce cas, les mobiles n'ont pas de capacité de traitement pour envoyer un message court SM avec une signature électronique ; par ailleurs, ces mobiles ont des capacités d'affichage faibles, qui ne permettent pas toujours un affichage confortable d'un message descriptif d'une offre, laquelle peut comprendre jusqu'à une centaine de caractères. Le procédé de l'invention comprend alors les échanges suivants, en plus de l'échange a) :

Echange b) : la passerelle P envoie au client un message fixe du type : "rappelez la passerelle au N°xxxxxxxx". Beaucoup de portables actuels ont une capacité de numérotation automatique d'un numéro reçu. Dans ce cas, il suffit d'appuyer sur une simple touche "appel" pour que le numéro xxxxxxxx soit appelé. Sinon, le client devra rentrer manuellement le numéro xxxxxxxx.

Echange c) : il est réalisé sous forme vocale entre la passerelle P, qui peut être un serveur audio et le portable. Ceci permet :

- d'authentifier le client en lui demandant un mot de passe préalablement convenu entre le client et l'opérateur de la passerelle P,

- de prendre connaissance de l'offre (ou des offres si il y en a plusieurs, et de choisir celle qui l'intéresse) ; pour ce faire :
  - la passerelle P traduira sous forme vocale l'offre reçue lors de l'échange a) grâce à un système de synthèse vocale,
  - le client pourra choisir cette offre et demander son paiement en appuyant, par exemple, sur la touche OK ou passer à l'offre suivante (touche #).

Echange d) : la passerelle P peut simplement confirmer au commerçant que le paiement a été fait.

Echange e) : la passerelle P ayant authentifié le client, et connaissant par ailleurs le numéro de carte bancaire de celui-ci, elle peut alors demander une autorisation aux banques si elle le juge nécessaire. On fait l'hypothèse que le client donne, lors de l'abonnement à ce service, son numéro de carte bancaire. D'autres procédés de paiement pourraient être utilisés : autorisation de prélèvement par exemple, que le client donnerait lors de l'abonnement.

Echange f) : le commerçant peut alors renvoyer une information particulière (exemples donnés plus haut) grâce au message f).

Echange g) : la passerelle P renvoie le message f) au client, sous forme de message court SM. La passerelle P peut mémoriser ces messages à des fins de levée de litiges entre client et commerçant, au cas où de tels litiges surviendraient ultérieurement.

Ce mode particulier de mise en oeuvre du procédé répond bien aux soucis de sécurité exposés plus haut. Il se fonde en effet sur une connaissance par la passerelle des clients et des commerçants :

- protection du numéro de carte bancaire : la variante décrite se fonde sur la correspondance entre un identifiant (numéro de téléphone du mobile) authentifiant par le mot de passe le numéro de carte bancaire dans la passerelle P (qui est une entité de confiance par définition). Le numéro de la carte bancaire peut être enregistré dans la passerelle lors de l'abonnement du client au service ;
- le commerçant doit s'authentifier auprès de la passerelle lors de l'échange a) ;
- l'engagement du client tient au fait que le client donne à la passerelle, entité de confiance, son mot de passe ; dans le cas de la variante décrite, le client accède à la passerelle en composant un numéro de téléphone mais aussi un code confidentiel ; celui-ci est à considérer aussi comme code d'accès au service délivré quand on est abonné.

2. Cas d'un équipement mobile de deuxième génération

On distinguera le cas où l'équipement mobile ne contient qu'une carte SIM et le cas où cet équipement contient une seconde carte du type carte bancaire.

2a. Cas d'un équipement mobile à une seule carte SIM

Dans ce cas, l'équipement mobile contient une carte à puce SIM capable d'enregistrer un programme dit SIM-TOOLKIT capable d'effectuer des traitements internes (calcul, gestion de données), d'agir sur l'affichage du mobile, de saisir les touches du clavier actionnées par l'utilisateur, de recevoir un message court, d'émettre un tel message, etc...

Dans ce cas, le système peut être ouvert, et comprendre plusieurs passerelles, qui ignorent les données propres aux équipements mobiles des clients. Chaque commerçant doit s'adresser à une passerelle particulière auprès de laquelle il est abonné.

Dans ce mode de mise en oeuvre :

- Le numéro de carte bancaire (PAN) est mémorisé dans le SIM ; il est transporté de façon sûre (confidentielle) jusqu'à la passerelle, dans l'échange c).
- Cet échange c) contient, de plus, une signature électronique qui va constituer une preuve de l'engagement du client dans cette transaction. A cet effet, le client doit préalablement fournir à la carte SIM un code confidentiel (CC) sans lequel celle-ci refuse de signer.
- L'authentification de la passerelle est assurée par un authentifiant donné par le message lors de l'échange b), et vérifié par le SIM ; la clé qui permet de vérifier cet authentifiant est la même que celle qui sert à chiffrer le PAN, et ceci garantit donc que seule une passerelle authentique est susceptible d'acquérir un PAN.

Dans un mode de mise en oeuvre avantageux, on utilise un système à clé publique avec arbre de certification. Cette évolution permet en effet de concevoir des systèmes simples, sûrs et ouverts. Cette technique est connue. On ne donnera donc que son mode d'application au présent procédé.

On désigne par A une autorité "racine" de l'arbre de certification qui certifie les différents serveurs de paiement. Elle certifie directement ou indirectement à travers une chaîne de certification à un ou plusieurs niveaux, les différents clients, donc en fait les clés secrètes et publiques (Si, Pi) qui sont dans le SIM et qui permettent de signer les ordres de télépaiement.

Dans l'échange b), le message contient alors l'identification de la passerelle, la date, l'identification du commerçant, l'identification du bien ou du service choisi, la description du bien ou du service choisi, la quantité, le prix, ... la clé publique de la passerelle, le certificat Cert(P) qui est le certificat de la passerelle attribué par l'entité A hiérarchiquement supérieure aux passerelles. Cert(P) est en fait la signature par cette autorité A de l'identité de la passerelle et de sa clé publique P : Cert(P)=SA (identités SP, P, ...). La clé publique PA correspondant à SA sera chargée dans tous les SIM "TOOLKIT" ayant cette application télépaiement.

A la réception du message, le programme de SIM va, à l'aide de PA, vérifier le certificat Cert(P) et donc obtenir P de façon sûre. Il va afficher un message "télépaiement" sur l'afficheur du portable. Le client pourra afficher les messages de l'offre, présents à cet instant : il obtient donc sur l'afficheur :

l'identification du commerçant, la description du bien choisi, la quantité, le prix.

Pour passer commande, donc payer, le client va introduire un code confidentiel CC que le SIM va comparer au CC interne qu'il mémorise. Si le code est correct, le SIM va envoyer le message c) contenant :

- l'ordre (avec la date, l'identification du commerçant, l'identification du bien ou du service choisi, la quantité, le prix, ...),
- les données de la carte chiffrées par la clé publique soit P(PAN),
- la signature de l'ordre de paiement Si (ordre de paiement),
- Pi, et les certificats de Pi.

Le message délivré à la passerelle dans l'échange c) parvient à la passerelle et celle-ci effectue les traitements suivants :

- vérification du certificat de Pi,
- vérification de la signature de l'ordre Si (ordre de paiement),
- déchiffrement de PAN par le calcul de S(P(PAN))=PAN pour obtenir le numéro de carte bancaire du client.

La passerelle ayant authentifié le client et connaissant, par ailleurs, le numéro de carte bancaire de celui-ci, elle peut alors demander une autorisation aux banques si elle le juge nécessaire (échange e)).

La passerelle peut simplement confirmer au commerçant que le paiement a été fait (d). Le commerçant peut alors renvoyer une information particulière (exemples donnés plus haut) grâce au message f)).

La passerelle renvoie le message au client, sous forme de message court SM. La passerelle mémorise ces messages à des fins de levée de litiges entre client et commerçant, au cas où de tels litiges surviendraient ultérieurement.

Ce mode de mise en oeuvre permet bien d'atteindre les objectifs visés, relativement à la sécurité :

- protection du numéro de carte bancaire : la variante décrite se fonde sur le chiffrement du PAN entre le mobile et la passerelle,
- le commerçant doit s'authentifier auprès de la passerelle de l'échange a). Par ailleurs, la passerelle est authentifiée indirectement par le mobile : plus exactement, si une fausse passerelle tentait de faire cette procédure, elle serait obligée, pour passer les tests de clés, d'emprunter la clé publique P et le certificat Cert(P) d'une passerelle authentique, et donc ne pourrait pas déchiffrer le PAN, ne connaissant pas la clé secrète correspondant à la clé publique P,
- l'engagement du client vient de ce que le client donne à la passerelle une signature Si (ordre de paiement) qui peut avoir une valeur juridique.

2b. Cas d'un équipement mobile à deux cartes

Dans ce cas, l'équipement mobile contient une carte SIM comme précédemment, mais encore un deuxième lecteur de carte adapté à la carte bancaire. Il est alors possible d'établir un dialogue avec cette seconde

carte. Les différents échanges peuvent alors être les suivants :

Echange n) : Cet échange préliminaire peut être effectué notamment :

- par contact téléphonique entre le client et le commerçant afin de négocier la transaction,
- par navigation et saisie sur le site Internet du commerçant,
- lors de ce premier contact la description du bien, le prix et les coordonnées du client sont enregistrées chez le commerçant.

Echange a) : l'offre du commerçant est envoyée à la passerelle afin d'être enregistrée et gérée jusqu'à la dernière étape de la transaction. Cette offre définit la prestation et contient des données d'identification du commerçant.

Echange b) : la passerelle authentifie le commerçant et transmet l'offre à l'équipement du client. Elle contient un numéro de transaction, la description du bien, le prix, etc... et les données d'identification de la passerelle.

Après ces échanges, l'application paiement disposée dans la carte SIM gère les échanges avec l'utilisateur de l'équipement en lui demandant de prendre une décision. Le client a alors la possibilité de confirmer son achat ou de ne pas donner suite. Si le client accepte l'offre qui lui est faite, l'application du SIM l'invite à introduire sa carte bancaire dans le second lecteur de carte de l'équipement GSM puis

l'invite à composer son code confidentiel. La suite des opérations est comparable à celle du paiement par carte bancaire avec un équipement tel qu'on les trouve dans les magasins.

Echange c) : l'équipement mobile GSM envoie à la passerelle P un message contenant les données du paiement bancaire, ou au contraire l'annulation de la commande.

Echange e) : en cas de confirmation de l'achat, la passerelle authentifie le client transmet les paramètres bancaires à la banque B.

Echange e') : la banque B examine la possibilité du paiement et en informe la passerelle P.

Echange d) : la passerelle adresse au commerçant l'information relative à la recevabilité du paiement.

Echange f) : le commerçant peut alors, éventuellement, ajouter des informations complémentaires (numéro de code d'une chambre d'hôtel, précision sur l'acheminement du bien, etc...). Il peut aussi annuler la transaction.

Echange g) : le client reçoit de la passerelle les paramètres bancaires de son achat (équivalent d'une facturette) et les éventuelles informations complémentaires du commerçant.

3. Equipement mobile avec application bancaire dans la carte SIM

A ces trois scenarii utilisant soit des mobiles de première génération (phase 1 ou phase 2), soit des mobiles de seconde génération (phase 2+), s'ajoute un quatrième scénario : le mobile doit être du type phase 2+ mais ne nécessite pas de lecteur supplémentaire pour la carte CB. L'application TK et les fonctions bancaires sont dans la carte SIM. Le déroulement des échanges est le même qu'avec une carte bancaire, si ce n'est que, dans le terminal du client, les échanges ne se font plus par l'intermédiaire d'un lecteur de carte bancaire puisque les fonctions de la carte bancaire sont intégrées dans la carte SIM.

REVENDICATIONS

1. Procédé de télépaiement impliquant une première entité dite "le client" (C) disposant d'un premier équipement téléphonique et une deuxième entité dite "le commerçant" (M) disposant d'un deuxième équipement de télécommunications, caractérisé en ce que l'équipement du client est un équipement téléphonique mobile et en ce qu'il implique en outre une troisième entité (P), dite "passerelle", disposant d'un troisième équipement de télécommunications apte à établir une liaison avec l'équipement du commerçant (M) et une liaison téléphonique avec l'équipement mobile du client (C), ce procédé comprenant les échanges suivants entre les équipements des trois entités :

a) le commerçant adresse à la passerelle (P) des données définissant une offre de prestation, avec notamment un montant à acquitter par le client, et ajoute à ces données des données d'identification du commerçant,

b) la passerelle (P) authentifie le commerçant, convertit les données de l'offre en un message adapté aux performances de l'équipement mobile du client (C) et adresse au client (C) ce message ainsi que des données d'authentification de la passerelle (P),

c) le client (C) authentifie la passerelle (P) et adresse en retour à celle-ci un message d'accord, ainsi que des informations permettant le paiement bancaire du montant de la prestation,

d) la passerelle (P) authentifie le client (C), vérifie que le paiement est possible et adresse

au commerçant (M) un message stipulant que le montant de la prestation est bien susceptible d'être acquitté.

2. Procédé selon la revendication 1, dans lequel, après l'échange d), le commerçant (M) renvoie à la passerelle (P) un message de confirmation et la passerelle (P) renvoie au client (C) un message de confirmation.

3. Procédé selon les revendications 1 ou 2, dans lequel la passerelle (P) ayant authentifié le client (C) elle demande à une banque (B) de vérifier si le montant de la prestation peut être acquitté et la banque (B) répond à la passerelle (P).

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel l'équipement mobile du client est un équipement de type GSM.

5. Procédé selon la revendication 4, dans lequel l'équipement mobile du client (C) comprend une carte d'identification (SIM) propre au client, laquelle carte contient un numéro de carte bancaire du client.

6. Procédé selon la revendication 5, dans lequel, au début de l'échange c), la carte d'identification (SIM) reçoit du client un code confidentiel (CC), vérifie si ce code est correct, et, si c'est le cas, la carte d'identification (SIM) chiffre le numéro de la carte bancaire du client à l'aide d'une clé, et l'équipement du client transmet à la passerelle (P) ce numéro chiffré.

7. Procédé selon la revendication 1, dans lequel le client authentifie la passerelle (P) au début de l'échange c) à l'aide d'une clé.

8. Procédé selon les revendications 6 et 7, dans lequel la clé servant à chiffrer le numéro de carte bancaire du client (C) et la clé servant à authentifier la passerelle (P) sont les mêmes.

9. Procédé selon la revendication 8, dans lequel la carte d'identification (SIM) du client (C) et la passerelle (P) possèdent chacune une clé secrète et une clé publique.

10. Procédé selon la revendication 1, dans lequel le client (C) signe le message d'accord transmis à la passerelle (P) lors de l'échange c) et la passerelle (P) authentifie cette signature.

11. Procédé selon la revendication 4, dans lequel l'équipement mobile du client (C) comprend une carte d'identification (SIM) et une seconde carte de type carte de paiement bancaire (CB).

12. Procédé selon la revendication 11, dans lequel, après avoir reçu de la passerelle (P) le message contenant les données relatives à l'offre du commerçant, la carte (SIM) invite le client à introduire sa carte bancaire (CB) dans l'équipement et à composer un code confidentiel.

13. Procédé selon la revendication 12, dans lequel l'équipement mobile du client (C) adresse à la passerelle (P) des données relatives au paiement bancaire, la passerelle (P) adresse ces données à une banque (B), qui examine la possibilité du paiement et en informe en retour la passerelle (P).

14. Procédé selon la revendication 12, dans lequel, après l'échange d) le commerçant (M) renvoie à la passerelle (P) un message de confirmation et la passerelle (P) renvoie au client (C) un message de confirmation.

15. Procédé selon la revendication 4, dans lequel lors des échanges b) et c), la passerelle (P) adresse au client (C) un message lui demandant de le rappeler, la passerelle (P) reçoit l'appel du client (C), authentifie le client (C) et lui adresse alors le message définissant l'offre de prestation faite par le commerçant (M).

16. Procédé selon la revendication 15, dans lequel, lors de l'échange c), le client (C) communique à la passerelle (P) un mot de passe et dans lequel, avant l'échange d), la passerelle (P) vérifie ledit mot de passe.

17. Procédé selon la revendication 4, dans lequel le commerçant (M) adresse son message d'offre vers une passerelle (P) particulière prise parmi plusieurs.

18. Système de télépaiement pour la mise en oeuvre du procédé selon la revendication 1, comprenant un

premier équipement téléphone mobile utilisé par un client (C), un deuxième équipement de télécommunications utilisé par un commerçant (M), un troisième équipement (P) de télécommunications utilisé par une passerelle apte à établir une liaison avec l'équipement du commerçant (M) et une liaison téléphonique avec l'équipement du client (C),

- l'équipement du commerçant (M) comprenant des moyens aptes à adresser à l'équipement de la passerelle (P) des données définissant une offre de prestation, avec notamment le montant à acquitter par le client (C) ainsi que des données d'identification du commerçant,
- l'équipement de la passerelle (P) comprenant des moyens d'authentification aptes à authentifier le commerçant (M) à partir des données d'identification de celui-ci et des moyens pour convertir les données de l'offre en un message adapté à l'équipement mobile du client (C) et pour adresser ce message au client avec des données d'identification,
- l'équipement mobile du client (C) comprenant des moyens pour authentifier la passerelle (P) et pour adresser à celle-ci un message d'accord ainsi que des informations confidentielles permettant le paiement du montant de la prestation,
- les moyens d'authentification de l'équipement de la passerelle (P) étant aptes en outre à authentifier le client (C), l'équipement de la passerelle (P) comprenant en outre des moyens pour s'assurer que le paiement est possible.

19. Système selon la revendication 18, dans lequel l'équipement mobile du client (C) est un équipement du type GSM.

20. Système selon la revendication 18, dans lequel l'équipement mobile du client (C) est pourvu de moyens permettant l'introduction et l'utilisation d'une carte de paiement bancaire (CB).

21. Système selon la revendication 18, dans lequel l'équipement mobile du client (C) est pourvu de moyens permettant l'introduction et l'utilisation d'un porte-monnaie électronique (PME).

1/1

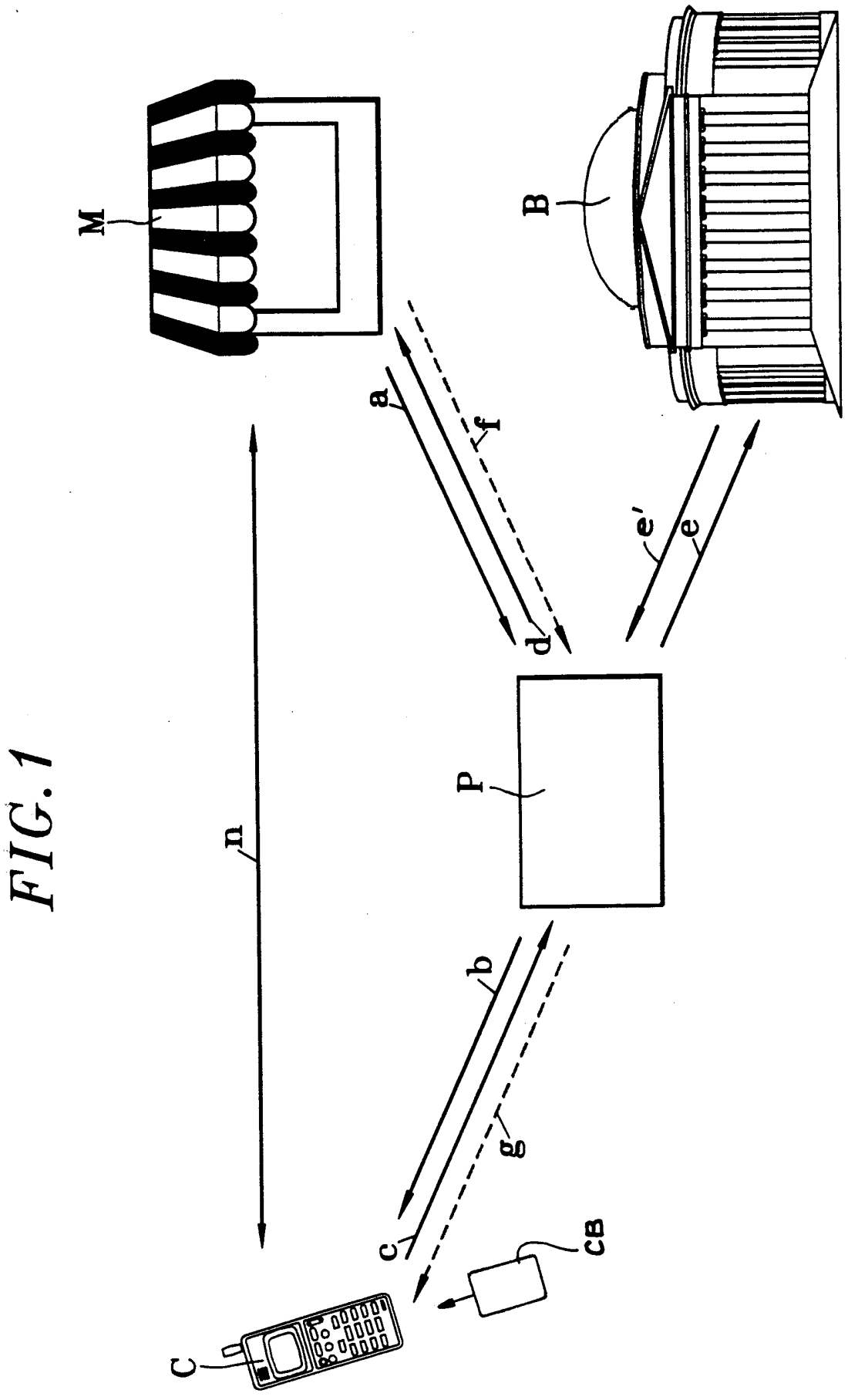


FIG. 1

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/FR 00/00412

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 H04Q7/32

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 H04Q 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 37524 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 27 August 1998 (1998-08-27) page 6, line 17 -page 11, line 3 page 12, line 25 -page 18, line 12 page 22, line 18 -page 26, line 6 figures 1,5-7 ---	1,4-7, 18,19
A	WO 96 25828 A (NOKIA MOBILE PHONES LTD ;TERHO MIKKO (FI); HEINONEN PETRI (FI); MA) 22 August 1996 (1996-08-22) ---	
A	WO 96 13814 A (VAZVAN BEHRUZ) 9 May 1996 (1996-05-09) ---	
A	WO 98 11519 A (SIEMENS AG ;VON BROCKDORFF CHRISTIAN FRIED (DE)) 19 March 1998 (1998-03-19) ---	
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] 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
11 May 2000	19/05/2000

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	Bocage, S

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/FR 00/00412

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 42173 A (LAHTI SEPPO ENSIO ;TELAMA SAMI PEKKA (FI); FD FINANSSIDATA OY (FI)) 1 October 1998 (1998-10-01)	

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/FR 00/00412

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9837524 A	27-08-1998	AU 6086898 A	09-09-1998
		AU 8007098 A	19-01-1999
		WO 9900773 A	07-01-1999
		EP 0992025 A	12-04-2000
		EP 0993664 A	19-04-2000
		NO 996147 A	28-02-2000
WO 9625828 A	22-08-1996	FI 950685 A	16-08-1996
		AU 696876 B	17-09-1998
		AU 4624796 A	04-09-1996
		AU 709016 B	19-08-1999
		AU 7865698 A	22-10-1998
		AU 712095 B	28-10-1999
		AU 7865798 A	15-10-1998
		CN 1174648 A	25-02-1998
		EP 0809916 A	03-12-1997
		JP 11501424 T	02-02-1999
		US 5887266 A	23-03-1999
WO 9613814 A	09-05-1996	FI 945075 A	29-04-1996
		EP 0739526 A	30-10-1996
		FI 962553 A	25-11-1997
		FI 962961 A	28-08-1996
		FI 971009 A	26-04-1997
		FI 971248 A	26-04-1997
		FI 971848 A	30-04-1997
WO 9811519 A	19-03-1998	CN 1225731 A	11-08-1999
		EP 0929880 A	21-07-1999
WO 9842173 A	01-10-1998	FI 971224 A	25-09-1998
		AU 6501998 A	20-10-1998
		EP 0972275 A	19-01-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/00412

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10 H04Q7/32

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 H04Q 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)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 98 37524 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 27 août 1998 (1998-08-27) page 6, ligne 17 -page 11, ligne 3 page 12, ligne 25 -page 18, ligne 12 page 22, ligne 18 -page 26, ligne 6 figures 1,5-7	1,4-7, 18,19
A	WO 96 25828 A (NOKIA MOBILE PHONES LTD ;TERHO MIKKO (FI); HEINONEN PETRI (FI); MA) 22 août 1996 (1996-08-22)	
A	WO 98 11519 A (SIEMENS AG ;VON BROCKDORFF CHRISTIAN FRIED (DE)) 19 mars 1998 (1998-03-19)	

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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'appartenant 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention 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
11 mai 2000	19/05/2000

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	Bocage, S

2

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem Internationale No
PCT/FR 00/00412

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	WO 98 42173 A (LAHTI SEPPO ENSIO ;TELAMA SAMI PEKKA (FI); FD FINANSSIDATA OY (FI)) 1 octobre 1998 (1998-10-01)	

2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem › Internationale No
PCT/FR 00/00412

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9837524 A	27-08-1998	AU 6086898 A	09-09-1998
		AU 8007098 A	19-01-1999
		WO 9900773 A	07-01-1999
		EP 0992025 A	12-04-2000
		EP 0993664 A	19-04-2000
		NO 996147 A	28-02-2000
WO 9625828 A	22-08-1996	FI 950685 A	16-08-1996
		AU 696876 B	17-09-1998
		AU 4624796 A	04-09-1996
		AU 709016 B	19-08-1999
		AU 7865698 A	22-10-1998
		AU 712095 B	28-10-1999
		AU 7865798 A	15-10-1998
		CN 1174648 A	25-02-1998
		EP 0809916 A	03-12-1997
		JP 11501424 T	02-02-1999
		US 5887266 A	23-03-1999
WO 9613814 A	09-05-1996	FI 945075 A	29-04-1996
		EP 0739526 A	30-10-1996
		FI 962553 A	25-11-1997
		FI 962961 A	28-08-1996
		FI 971009 A	26-04-1997
		FI 971248 A	26-04-1997
		FI 971848 A	30-04-1997
WO 9811519 A	19-03-1998	CN 1225731 A	11-08-1999
		EP 0929880 A	21-07-1999
WO 9842173 A	01-10-1998	FI 971224 A	25-09-1998
		AU 6501998 A	20-10-1998
		EP 0972275 A	19-01-2000