(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
3 janvier 2002 (03.01.2002)

PCT

(10) Numéro de publication internationale
WO 02/01432 A1

(51) Classification internationale des brevets[7] : G06F 17/60

(21) Numéro de la demande internationale :
PCT/FR01/02013

(22) Date de dépôt international : 26 juin 2001 (26.06.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/08138 26 juin 2000 (26.06.2000) FR

(71) Déposant et
(72) Inventeur : GALKA, Radoslaw [PL/FR]; 15, allée des Pastoureaux, F-91210 Draveil (FR).

(74) Mandataire : ABELLO, Michel; Cabinet Peuscet, 78, avenue Raymond Poincaré, F-75116 Paris (FR).

(81) États désignés *(national)* : PL, RU, US.

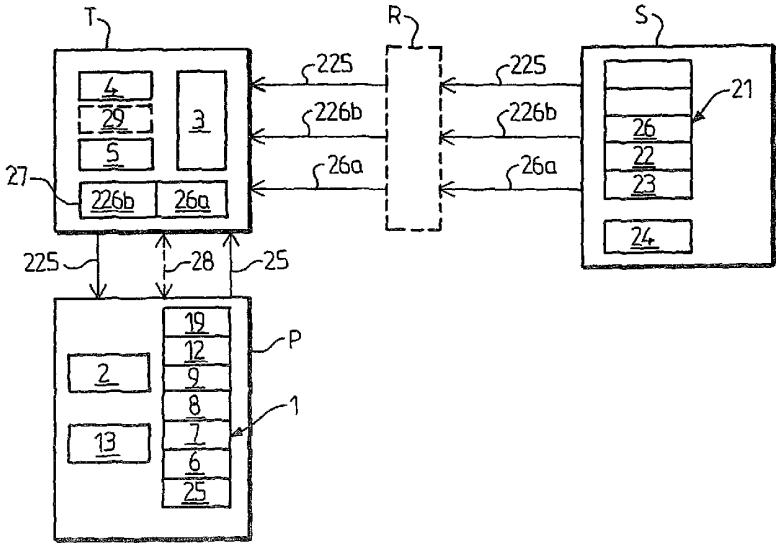
(84) États désignés *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Publiée :
— *avec rapport de recherche internationale*

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.

(54) Title: METHOD FOR ONLINE COMMERCIAL DISTRIBUTION OF DIGITAL GOODS THROUGH A COMMUNICATION NETWORK AND ELECTRONIC DEVICE FOR PURCHASING ELECTRONIC GOODS DISTRIBUTED BY SAID METHOD

(54) Titre : PROCEDE DE DISTRIBUTION COMMERCIALE EN LIGNE DE BIENS NUMERIQUES PAR L'INTERMEDIAIRE D'UN RESEAU DE COMMUNICATION ET DISPOSITIF ELECTRONIQUE D'ACHAT DE BIENS NUMERIQUES DISTRIBUES PAR CE PROCEDE



(57) Abstract: The invention concerns a method for distributing digital goods via a communication network (R), comprising steps which consist in: (a) connecting with a terminal (T), electronic payment means (P); (b) following an order instruction made by said client to the purchase terminal to order a digital good of his choice, sending said credit data (7) to a supplier server, (d) sending, from the server to the purchase terminal said digital good (26) comprising a file of digital data executable or not. The invention is characterised in that said digital good comprises a separate file of rights to use (225) defining terms and conditions of use of the digital good selected by the client, said method comprising steps which consist in: (f) storing in said storage (1) of the electronic payment means said data concerning rights to use (25).

[Suite sur la page suivante]

WO 02/01432 A1

(57) Abrégé : Procédé de distribution commerciale de biens numériques par l'intermédiaire d'un réseau de communication (R), comprenant les étapes consistant à : (a) mettre en communication avec un terminal d'achat (T), un moyen électronique de paiement (P) ; (b) à la suite d'un ordre de commande donné par ledit client au terminal d'achat pour commander un bien numérique de son choix, envoyer lesdites données de crédit (7) à destination d'un serveur d'un fournisseur ; (d) envoyer, depuis le serveur à destination d'un terminal d'achat, ledit bien numérique (26) comprenant un fichier de données numériques exécutable ou non, caractérisé par le fait que ledit bien numérique comprend un fichier séparé de données de droits d'utilisation (225) définissant les modalités d'utilisation du bien numérique choisies par le client, ledit procédé comportant les étapes consistant à : (f) mémoriser dans ladite mémoire (1) du moyen électronique de paiement lesdites données de droits d'utilisation (25).

PROCEDE DE DISTRIBUTION COMMERCIALE EN LIGNE DE BIENS NUMERIQUES PAR L'INTERMEDIAIRE D'UN RESEAU DE COMMUNICATION ET DISPOSITIF ELECTRONIQUE D'ACHAT DE BIENS NUMERIQUES DISTRIBUES PAR CE PROCEDE

La présente invention concerne un procédé de distribution commerciale de biens numériques par l'intermédiaire d'un réseau de communication; ainsi qu'un dispositif électronique pour acheter des biens numériques par l'intermédiaire d'un réseau de communication et un système d'achat en ligne prêt à installer. Plus précisément, les biens numériques concernés par l'invention sont des ensembles de données numériques exécutable(s) destinés à être utilisé et devant être fournis sous une forme utilisable selon des modalités prédéfinies d'utilisation.

Les réseaux ouverts de communication ou de transport de données, comme l'Internet, présentent de très grandes potentialités pour le commerce. Le commerce électronique, terme qui désigne les transactions commerciales en ligne par l'intermédiaire de l'Internet, est appelé à une très forte croissance à cause de la croissance du nombre d'utilisateurs de l'Internet, et des nombreux avantages qu'il présente : possibilité d'acheter et de vendre en tout point du globe, rapidité qui favorise la réduction des stocks. Particulièrement, le commerce électronique apparaît très avantageux pour le commerce de biens transportables sous forme numérisée, enregistrement audio et/ ou vidéo, disques films, logiciels, textes, images, etc. puisqu'il réduit considérablement les frais de distribution par rapport aux circuits classiques. Cependant, la sécurité des échanges sur un tel réseau ouvert, c'est-à-dire sur lequel les échanges entre deux interlocuteurs peuvent être lus par un tiers, est plus complexe à assurer.

Actuellement, la méthode d'authentification et de paiement la plus répandue pour sécuriser les transactions en ligne sur l'Internet repose sur protocole SSL (en anglais, Secure Socket Layer.) SSL est un protocole de communication d'informations qui permet d'assurer l'authentification des interlocuteurs, la confidentialité des communications, et l'intégrité des données échangées sur l'Internet. Ce protocole utilise un moyen de cryptographie reconnu : l'algorithme à clé publique RSA. Une clé RSA est un couple formé d'une

clé publique et d'une clé privée, qui est le résultat d'opération entre nombres premiers. Tout message encodé avec la clé publique d'un couple ne peut être lu qu'avec la clé privée dudit couple.

En référence à la figure 1, le passage d'une commande d'achat à l'aide du protocole SSL par un client C, ayant un terminal T apte à communiquer avec un serveur S d'un fournisseur F par l'intermédiaire d'un réseau ouvert R, va maintenant être décrit. Avant que les informations sensibles ne soient échangées, le protocole SSL effectue la gestion des clés RSA et l'authentification du serveur. Pour authentifier le serveur S d'un site de commerce électronique sur la Toile (le web), le logiciel d'achat L, exécuté sur le terminal informatique T par le client C, demande au serveur S de lui fournir sa clé publique 30. Le terminal T reçoit la clé publique 30 du serveur S, puis encode la clé publique 31 générée par le logiciel L avec la clé publique 30 du serveur S, et retourne au serveur S le produit de cette opération, la clé encodée 131. Seul le serveur S possède la clé privée 32 correspondant à la clé publique 30. Ainsi, le serveur S décode la clé 131 pour obtenir la clé publique 31 du logiciel L. Le serveur S encode ses messages pour le logiciel d'achat L avec la clé publique 31, de sorte que seul le logiciel L peut décoder ces messages, à l'aide la clé privée 33 correspondant à la clé publique 31. Un tiers ayant observé l'échange ne peut pas décoder la clé 131, et ne peut donc pas se faire passer pour le serveur S auprès du logiciel L. En répétant cette procédure, en commençant cette fois par le serveur S, le serveur S peut authentifier le logiciel L du client C. Ainsi, les deux interlocuteurs peuvent communiquer de manière confidentielle.

Lorsque le client C veut passer une commande d'achat d'un bien B, le logiciel L l'invite à saisir des paramètres de paiement 34 sur un clavier 35. Les paramètres de paiement comportent généralement le nom, l'adresse du client C, le numéro d'une carte de paiement, son type (par exemple, VISA®, American Express®) et sa date d'expiration. Le logiciel L chiffre ces données et transmet les paramètres de paiement chiffrés 134 au serveur S. Le fournisseur F procède alors à la vérification des paramètres de paiement 34 et confirme la commande par un message au client C, ledit message

pouvant comporter une facture. Le bien B peut alors être livré par colis postal par exemple.

Une autre méthode d'authentification des personnes impliquées lors d'un achat en ligne est le protocole SET (en anglais, Secure Electronic Transaction®.) Ce système utilise des protocoles de cryptographie et délivre des certificats d'authenticité des transactions électroniques.

L'une comme l'autre des méthodes SSL et SET comporte des inconvénients, dont leur lourdeur et leur rigidité. Dans le protocole SSL, les paramètres de paiement doivent être saisis à chaque transaction, avec les risques que suppose une telle saisie, si elle est effectuée dans un lieu public. La solution SET est lourde à mettre en œuvre à cause des certificats d'authenticité qui doivent être échangés à chaque transaction.

Le document EP 917 119 A2 expose un système réticulaire distribué de portefeuille électronique comportant une banque d'information dans laquelle un utilisateur stocke différents types d'informations personnelles et une carte à puce contenant des connecteurs secrets pour autoriser un accès nomade ubiquiste de l'utilisateur à ces informations tout en garantissant leur confidentialité. Dans ce système, des données de crédit de l'utilisateur sont stockées de manière permanente dans la banque d'information pour permettre une facturation interne à la banque d'information. Ainsi, l'utilisateur peut effectuer des achats sur des sites marchands de l'Internet par l'intermédiaire de la banque d'information sans faire passer d'informations telles qu'un numéro de carte bancaire par l'Internet. Ce système prévoit aussi de stocker sur la carte à puce un ticket d'accès, par exemple une entrée à l'opéra. Cependant, ce système comporte des inconvénients en ce qu'il rend l'utilisateur entièrement dépendant de la banque d'information, qui centralise toutes ses données personnelles et sert toujours d'intermédiaire pour les transactions effectuées par l'utilisateur avec des tiers. Ainsi, ce système prive l'utilisateur d'un contrôle souhaitable sur ses propres affaires. En outre, la centralisation des données personnelles est un facteur de risque pour l'utilisateur. Enfin, la banque d'information doit être rémunérée pour ses services d'intermédiaire.

La distribution commerciale en ligne de biens numériques par l'intermédiaire d'un réseau de communication est une forme particulière de transaction commerciale en ligne. L'achat des biens numériques en ligne par l'intermédiaire d'un réseau de communication est une forme particulière de commande commerciales en ligne. Le document WO 99/49615 A1 expose un procédé de distribution commerciale en ligne de biens numériques par l'intermédiaire d'un réseau de communication, ledit procédé comprenant les étapes consistant à :

(a) mettre en communication de manière amovible avec un premier terminal informatique, dit terminal d'achat, un moyen électronique de paiement destiné à être porté par un client, des données de crédit identifiant un crédit dudit client étant mémorisées dans une mémoire dudit moyen électronique de paiement,

(b) à la suite d'un ordre de commande donné par ledit client au terminal d'achat pour commander un bien numérique de son choix, envoyer lesdites données de crédit depuis le terminal d'achat à destination d'un second terminal informatique, dit serveur, d'un fournisseur, lesdites données de crédit étant chiffrées, ledit serveur et ledit terminal d'achat étant aptes à communiquer par l'intermédiaire dudit réseau de communication,

(c) vérifier la validité desdites données de crédit et, lorsque lesdites données de crédit sont valides,

(d) envoyer, depuis le serveur à destination du terminal d'achat, ledit bien numérique comprenant au moins un fichier de données numériques exécutable(s) ou non.

Selon ce procédé connu, le fichier de données, par exemple un document numérisé est mémorisé de manière chiffrée sur une cartouche de stockage pour laquelle, d'une part, le terminal d'achat, d'autre part, l'ordinateur personnel du client, doivent être munis d'un lecteur spécifique. A des fins de protection contre le piratage, un seul lecteur ou un ensemble restreints de lecteurs, dont les numéros de série ont été entrés dans la cartouche, permet l'utilisation du bien numérique mémorisé dedans. Le moyen de paiement est une carte bancaire classique, à piste magnétique ou autre, et le client doit posséder en outre une carte d'identification personnelle séparé de la

carte bancaire pour pouvoir utiliser le terminal d'achat. Ce procédé et ce système présentent donc une certaine lourdeur d'utilisation. La nécessité de posséder à la fois une carte de paiement, une carte d'identification et une cartouche de stockage pour réaliser un achat rend ce dernier fastidieux et accroît les risques qu'un achat souhaité ne puisse être réalisé à cause de l'oubli de l'un de ces trois éléments. De plus, le bien acheté est dépourvu de flexibilité d'utilisation car l'utilisation ne s'effectue pas depuis le terminal d'achat et le lecteur adapté à la cartouche doit être apporté avec la cartouche sur tout lieu d'utilisation.

La présente invention a pour but de proposer un procédé de distribution commerciale de biens numériques par un réseau en résolvant au moins certains des inconvénients précités. Le procédé selon l'invention apporte cinq avantages majeurs aux clients : l'automatisation et la sécurisation du processus de paiement par l'utilisation d'une carte à puce et d'un lecteur approprié ; l'ouverture à toute carte de paiement valide ; la personnalisation de la gamme de produits commercialisés en ligne et la personnalisation des messages publicitaires grâce à une gestion dynamique des préférences du client mémorisées dans la carte à puce ; l'acheminement direct des biens numériques tels que les logiciels, enregistrements audio et/ou vidéo achetés, par téléchargement, sur le terminal du client, de fichiers électroniques chiffrés ou non contenant ces produits sous une forme utilisable uniquement par l'intermédiaire de la carte à puce.

Pour cela, l'invention fournit un procédé du type ci-dessus, caractérisé par le fait que ledit bien numérique comprend un fichier séparé de données de droits d'utilisation définissant des modalités d'utilisation du bien numérique choisies par le client et un ou plusieurs autre(s) fichier(s) de données, lesdites données de droits d'utilisation étant envoyées chiffrées selon un code de chiffrement pour lequel une clé de déchiffrement secrète est mémorisée dans la mémoire dudit moyen électronique de paiement, ledit procédé comportant les étapes consistant à :

(e) mémoriser ledit ou lesdits autre(s) fichier(s) de données sur le terminal d'achat,

(f) mémoriser dans ladite mémoire du moyen électronique de paiement

lesdites données de droits d'utilisation en les déchiffrant à l'aide de ladite clé de déchiffrement, lesdites données de droits d'utilisation étant indispensables à l'utilisation dudit bien numérique.

Par exemple, le moyen électronique de paiement est une carte à puce apte à exécuter des algorithmes cryptographiques et le terminal d'achat est un micro-ordinateur équipé d'un lecteur de carte à puce. Une telle carte à puce est munie d'une mémoire, par exemple d'une capacité de 32 Kilo-octets ou plus. Le serveur est par exemple le serveur d'un site ou d'un portail de commerce électronique sur la Toile.

Ce procédé permet ainsi de réaliser des achats directement auprès de fournisseurs sans passer par une quelconque institution intermédiaire. Il offre une sécurité contre le piratage dans le mesure où le moyen de paiement ayant servi à réaliser l'achat doit être relié à l'interface pour permettre l'utilisation du bien acquis. Mais il offre aussi une flexibilité d'utilisation puisque le ou les autre(s) fichier(s) peut/peuvent être transféré(s) ou copié(s), par exemple via le réseau de communication, sur un autre terminal muni d'une interface adaptée au moyen de paiement. Il ne nécessite pas de précautions particulières contre le piratage lors d'un tel transfert puisque seul le moyen de paiement connecté à une interface permet d'utiliser le bien depuis un terminal. Il est à noter qu'un terminal informatique muni d'un lecteur de carte à puce est un objet relativement courant.

Avantageusement, ledit ordre de commande produit l'envoi par le terminal d'achat, à destination du serveur, de données de commandes désignant ledit bien numérique choisi par le client et les modalités d'utilisation choisies par le client, selon lesquelles ledit bien numérique est destiné à être utilisé, les données de droits d'utilisation étant destinées à autoriser une utilisation dudit bien numérique selon lesdites modalités d'utilisation choisies.

Dans un mode de réalisation préféré, le ou les autre(s) fichier(s)comprend/comprennent un programme d'ordinateur exécutable, ladite utilisation comportant une exécution dudit programme d'ordinateur, ledit programme d'ordinateur étant conçu de manière que son exécution comporte des opérations non soumises à autorisation consistant à lire les données de droits d'utilisation dans

ledit moyen électronique de paiement et à autoriser ou non, en fonction desdites données de droits d'utilisation, l'exécution d'au moins une opération suivante soumise à autorisation.

Dans un autre mode de réalisation préféré, le ou les autre(s) fichier(s)comprend/comprennent au moins un fichier de document non exécutable, ladite utilisation comportant des opérations non soumises à autorisation consistant à lire les données de droits d'utilisation dans ledit moyen électronique de paiement et à autoriser ou non, en fonction desdites données de droits d'utilisation, l'exécution d'au moins une opération de traitement dudit ou desdits fichier(s) de document par un moyen de traitement correspondant.

Dans une combinaison de ces mode de réalisation préférés, ledit programme d'ordinateur exécutable par ledit terminal d'achat constitue ledit moyen de traitement, ladite ou lesdites opération(s) suivante(s) comportant ladite ou lesdites opération(s) de traitement dudit ou desdits fichier(s) de document.

De préférence, le procédé selon l'invention comporte une étape consistant à :

(g) chiffrer au moins partiellement ledit ou lesdits autre(s) fichier(s) de données selon ledit code de chiffrement avant de le(s) mémoriser sur le terminal d'achat, ledit procédé comportant une étape de déchiffrement de la partie chiffrée dudit ou desdits autre(s) fichier(s) de données par ledit moyen électronique de paiement lorsqu'une utilisation du bien numérique est ordonnée. La partie chiffrée peut aussi être vide.

Le stockage d'au moins une partie du bien numérique sous une forme chiffrée sur le terminal d'achat et de la clé de déchiffrement correspondante sur un moyen de paiement amovible offre une garantie supplémentaire contre le piratage du bien numérique.

Avantageusement, le procédé selon l'invention comporte, avant l'étape (a), une étape consistant à fournir au client le moyen électronique de paiement avec des clés de chiffrement et de déchiffrement incluses et pour lesquelles clés le fournisseur possède des clés de déchiffrement et de chiffrement respectives correspondantes.

Avantageusement, le procédé selon l'invention comprend aussi une étape d'authentification mutuelle qui comporte, d'une part,

l'envoi par ledit moyen électronique de paiement, à destination dudit second terminal informatique, par l'intermédiaire dudit premier terminal informatique et dudit réseau de communication, d'un nombre aléatoire, d'autre part, le renvoi par ledit second terminal informatique, à destination dudit moyen électronique de paiement, par l'intermédiaire dudit réseau de communication et dudit premier terminal informatique, dudit nombre aléatoire reçu, après chiffrement à l'aide d'une clé d'authentification dudit second terminal informatique, une condition nécessaire à la reconnaissance d'authenticité dudit second terminal informatique par ledit moyen électronique de paiement étant la réception dudit nombre aléatoire chiffré par ledit moyen électronique de paiement et la concordance entre ledit nombre aléatoire envoyé et ledit nombre aléatoire chiffré, après déchiffrement de ce dernier par ledit moyen électronique de paiement.

De préférence, les modalités d'utilisation définies par lesdites données de droits d'utilisation comportent des modalités chronologiques comme une durée maximale d'utilisation ou une date limite d'utilisation, et/ou des modalités quantitatives comme un nombre maximal d'utilisations, et/ou des modalités qualitatives comme une restriction de l'utilisation à un sous-ensemble dudit bien numérique.

L'invention fournit également un dispositif électronique pour acheter des biens numériques en ligne par l'intermédiaire d'un réseau de communication, ledit dispositif comprenant :

- un moyen électronique de paiement destiné à être porté par un client et muni d'une mémoire, des données de crédit identifiant un crédit dudit client étant mémorisées dans ladite mémoire,
- un terminal informatique d'achat relié à un serveur informatique dudit fournisseur par ledit réseau de communication, et muni d'une interface de commande pour recevoir un ordre de commande donné par le client pour commander un bien numérique de son choix,
- une interface électronique reliée audit terminal d'achat, ladite interface électronique étant apte à recevoir de manière amovible ledit moyen électronique de paiement pour permettre un échange de données entre ledit terminal d'achat et ledit moyen électronique de paiement,
- des moyens logiciels de pilotage pour piloter les opérations consistant à :

(a) envoyer lesdites données de crédit depuis ledit moyen électronique de paiement à destination dudit serveur, lesdites données de crédit étant chiffrées,

(b) lorsque lesdites données de crédit ont été validées, recevoir depuis le serveur ledit bien numérique comprenant au moins un fichier de données exécutable ou non,

caractérisé par le fait que ledit bien numérique comporte un fichier séparé de données de droits d'utilisation définissant des modalités d'utilisation du bien numérique choisies par le client et un ou plusieurs autre(s) fichier(s) de données, lesdites données de droits d'utilisation étant reçues chiffrées, lesdits moyens logiciels de pilotage étant aptes à piloter les opérations consistant à :

(c) mémoriser ledit ou lesdits autre(s) fichier(s) de données sur le terminal d'achat,

(d) mémoriser lesdites données de droits d'utilisation dans ladite mémoire du moyen électronique de paiement en les faisant déchiffrer par le moyen électronique de paiement à l'aide d'une clé de déchiffrement secrète mémorisée dans sa mémoire, lesdites données de droits d'utilisation étant indispensables à l'utilisation dudit bien numérique.

Par exemple, le moyen électronique de paiement est une carte à puce apte à exécuter des algorithmes cryptographiques et l'interface électronique de paiement est un lecteur de carte à puce dans lequel ladite carte à puce peut être insérée.

De préférence, ladite interface de commande permet au client d'ordonner une utilisation dudit bien numérique.

De préférence, ledit ou lesdits autre(s) fichier(s) de données est/sont reçu(s) au moins partiellement chiffré(s) selon ledit code de chiffrement, lesdits moyens logiciels de pilotage étant aptes à piloter une opération consistant à faire déchiffrer la partie chiffrée dudit ou desdits autre(s) fichier(s) de données par le moyen électronique de paiement à l'aide de ladite clé de déchiffrement secrète lorsque ladite utilisation est ordonnée.

L'invention fournit également un système d'achat en ligne prêt à installer comportant ledit moyen électronique de paiement, ladite interface électronique et lesdits moyens logiciels de pilotage du

dispositif électronique susmentionné, ledit moyen électronique de paiement étant ou non relié à ladite interface électronique, ladite interface électronique étant ou non reliée audit terminal d'achat et lesdits moyens logiciels étant fixés sur un support de données.

L'invention sera mieux comprise, et d'autres buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description suivante de plusieurs modes de réalisation particuliers de l'invention, donnés uniquement à titre illustratif et non limitatif, en référence au dessin annexé. Sur ce dessin :

- la figure 1 est une représentation schématique d'une procédure pour effectuer un achat par l'intermédiaire d'un réseau de communication selon un art antérieur ;
- la figure 2 est une représentation schématique d'une étape d'initialisation d'une carte à puce faisant partie d'un procédé selon l'invention ;
- la figure 3 est une représentation schématique d'une première étape d'achat du procédé de la figure 2 ;
- la figure 4 est une représentation schématique d'une seconde étape d'achat du procédé de la figure 2 ;
- la figure 5 est un diagramme représentant le déroulement d'une utilisation du bien numérique acquis par le procédé des figures 2 à 4 dans un premier mode de réalisation ;
- la figure 6 est un diagramme représentant le déroulement d'une utilisation du bien numérique dans un second mode de réalisation.

Un dispositif électronique selon un mode de réalisation de l'invention va maintenant être décrit en référence à la figure 2. Le dispositif électronique dans ce mode de réalisation de l'invention comprend une carte à puce P, qui comporte par exemple une armature de plastique rigide (non représentée) dans laquelle est monté un circuit intégré avec une unité de mémoire 1, un microprocesseur 2, et des contacts électriques (non représentés) apte à entrer en contact avec un lecteur de carte à puce pour permettre l'échange de données entre la carte à puce P et ledit lecteur. Le dispositif selon l'invention comprend aussi un lecteur de carte à puce 3, relié à un terminal informatique T pour échanger des données avec celui-ci. Comme représenté à la figure

2, le lecteur de carte à puce 3 peut être intégré au terminal T. En variante, le lecteur de carte à puce 3 peut être un périphérique externe au terminal T. Le dispositif selon l'invention comprend également des moyens logiciels 4, qui comportent des codes d'instructions aptes à être exécutés par le terminal T et/ou le lecteur de carte à puce 3 pour piloter le déroulement d'un procédé d'achat. Les moyens logiciels 4 sont installés sur le terminal T et/ou le lecteur de carte à puce 3 par tout moyen approprié, soit par l'intermédiaire d'un support physique de données de type cédérom (non représenté), soit par téléchargement.

La carte à puce P, le lecteur 3 et les moyens logiciels 4 peuvent être fournis sous forme d'un système prêt à installer sur un ordinateur personnel classique, tel qu'un micro-ordinateur de type compatible PC. Les moyens logiciels 4 sont alors fournis fixés sur un support physique de données. Le lecteur 3 est fourni avec un cordon pour le relier audit ordinateur personnel. Le procédé piloté par les moyens logiciels de pilotage 4 va maintenant être décrit.

Dans une première étape du procédé, un client C initialise sa carte à puce P pour la rendre utilisable afin d'effectuer des transactions en ligne. Pour cela, la carte à puce P est insérée dans le lecteur de carte à puce 3. Une application d'initialisation, fournie dans les moyens logiciels 4, est exécutée. Le client C est alors invité à saisir différentes informations le concernant par l'intermédiaire d'une interface de commande 5, par exemple un clavier alphanumérique et/ou une souris, du terminal T. Ces différentes informations comportent par exemple : des données personnelles 6 identifiant le client C (par exemple, son nom, son adresse, sa date de naissance), des données bancaires ou autres 7 identifiant un crédit du client C (par exemple, un numéro de carte bancaire du client C, le type de ladite carte bancaire et sa date d'expiration), des données de préférences personnelles 8, caractéristiques des préférences de consommation du client C (adresse d'un site de commerce électronique préféré, nom de marques commerciales et/ou de distributeurs préférés, etc.) A la fin de la saisie de ces informations, le client C est invité à fournir un code d'identification personnel 9 ; puis le lecteur 3 transmet les données personnelles 6, les données bancaires 7, les données de préférences personnelles 8 et le code d'identification personnel 9 à la carte à puce

P, pour que ces informations soient mémorisées dans l'unité de mémoire 1. L'étape d'initialisation est alors terminée.

De préférence, le client C doit garder secret son code d'identification personnel 9, pour se réserver l'accès aux informations mémorisées sur sa carte à puce. Le code d'identification personnel 9 est nécessaire pour visualiser et/ou modifier lesdites informations mémorisées à l'aide de l'application d'initialisation. Le code d'identification personnel 9 est bien entendu complètement indépendant d'autres codes personnels appartenant au client C, comme par exemple le code confidentiel associé à sa carte bancaire.

Pendant l'étape d'initialisation, qui doit être effectuée au moins avant le tout premier achat à l'aide de la carte à puce P, il n'est pas nécessaire que le terminal T soit connecté à un quelconque réseau. De plus, la saisie des données sensibles, comme les données bancaires 7, peut être effectuée dans un lieu approprié, et non sur le lieu où est réalisé l'achat, qui peut être dans un lieu public, comme un cybercafé par exemple.

Après cette étape d'initialisation, le dispositif électronique permet au client C d'effectuer des achats en ligne auprès d'un fournisseur F par l'intermédiaire d'un réseau de communication R, comme représenté aux figures 3 et 4. Pour cela, le terminal T doit être relié au réseau R afin de communiquer avec un serveur informatique S du fournisseur F, également relié au réseau R. Le serveur S est, par exemple, le serveur d'un site de commerce électronique sur la Toile. Dans la suite, les communications entre le serveur S et le terminal T passent toujours par le réseau R. Le réseau R est un réseau ouvert du type de l'Internet, c'est-à-dire qu'un tiers pourrait intercepter les données échangées entre le serveur S et le terminal T.

Pour effectuer un achat, le client C insère sa carte à puce P dans le lecteur 3. Le terminal T est alors apte à entrer automatiquement en communication avec le serveur S du site de commerce électronique dont l'adresse figure dans les données de préférences 8 mémorisées dans la carte à puce P. En variante, le client C peut choisir un serveur S différent en saisissant son adresse par l'interface de commande 5.

Lorsque le terminal T est entré en communication avec le serveur S, les deux interlocuteurs informatiques S et T s'identifient mutuellement lors d'une étape d'authentification, effectuée selon une procédure d'authentification standard mise en place pour les cartes à puce cryptographiques, transparente pour le client C, comme par exemple l'algorithme à clé publique RSA susmentionné.

Pour la procédure d'authentification (non représentée), le serveur S possède une paire de clés d'authentification, l'une publique 36, l'autre privée 37. Le serveur S révèle sa clé d'authentification publique 36 au terminal T sans passer par le réseau R. Le terminal T génère un nombre aléatoire 38 et l'envoie au serveur S par l'intermédiaire du réseau R. Le serveur S chiffre ce nombre aléatoire 38 reçu à l'aide de sa clé d'authentification privée 37, et retourne le résultat 39 de cette opération de chiffrement au terminal T. Le terminal T utilise la clé d'authentification publique 36 révélée précédemment pour déchiffrer le résultat 39 reçu et compare ledit résultat déchiffré 40 au nombre aléatoire 38 envoyé. S'ils correspondent, le terminal T est assuré de correspondre avec le serveur S. Un imposteur n'aurait pu connaître la clé d'authentification privée 37 du serveur S et serait incapable de chiffrer correctement le nombre aléatoire 38.

A l'issue de l'étape d'authentification, le terminal T est apte à envoyer au serveur S des données chiffrées selon un premier code de chiffrement, que seul le serveur S est apte à déchiffrer, à l'exclusion de tout tiers qui observerait les échanges sur le réseau R entre le terminal T et le serveur S ; et le serveur S est apte à envoyer au terminal T des données chiffrées selon un second code de chiffrement que seul le terminal T muni de la carte à puce P est apte à déchiffrer, à l'exclusion de tout tiers. Aux figures 3 et 4, les données chiffrées selon le premier code de chiffrement ont un chiffre augmenté de 100 et les données chiffrées selon le second code de chiffrement ont un chiffre de référence augmenté de 200.

La carte à puce P comporte dans l'unité de mémoire 1 une dite seconde clé de déchiffrement 12 nécessaire au déchiffrement dudit second code de chiffrement, ainsi qu'une première clé de chiffrement 19 nécessaire au chiffrement selon le premier code de chiffrement. Ainsi, le terminal T ne peut, ni déchiffrer ledit second code de

chiffrement, ni chiffrer des données selon ledit premier code de chiffrement, lorsque la carte à puce P est retirée du lecteur 3. Les opérations de chiffrement selon le premier code des données envoyées par le terminal T au serveur S et de déchiffrement des données envoyées au terminal T par le serveur S chiffrées selon le second code de chiffrement sont effectuées par un module cryptographique 13 dans la carte à puce P. Le serveur S comporte un second module cryptographique 24 pour chiffrer selon le second code à l'aide d'une seconde clé de chiffrement 23, et pour déchiffrer le premier code à l'aide d'une première clé de déchiffrement 22, lesdites seconde clé de chiffrement 23 et première clé de déchiffrement 22 étant mémorisées dans une mémoire 21 du serveur S.

La clé de chiffrement 19 correspondant au premier code et la clé de déchiffrement 12 correspondant au second code sont fixées dans la carte à puce P sans passer par le réseau R. Par exemple, le fournisseur F est lui-même l'émetteur de la carte à puce de sorte qu'il la fournit au client C avec les clés 19 et 12 intégrées. Par exemple, dans le cas où l'algorithme à clé publique RSA est utilisé pour l'authentification mutuelle des interlocuteurs, la seconde clé de chiffrement 23 est une clé publique générée par la carte à puce P et la seconde clé de déchiffrement 12 est la clé privée qui lui est associée ; tandis que la première clé de chiffrement 19 est une clé publique générée par le serveur S et la première clé de déchiffrement 22 est la clé privée qui lui est associée.

Après l'étape d'authentification, le terminal T envoie au serveur S les données de préférences 8 chiffrées selon le premier code de chiffrement. Après réception des données de préférences chiffrées 108, le serveur S envoie au terminal T des données de réponse 10, chiffrées ou non, destinées à informer et/ou influencer le client C. Les données de réponse 10 comportent par exemple des informations sur des produits conformes aux données de préférences 8, des annonces publicitaires et/ou des offres commerciales personnalisées selon les données de préférences 8.

Le fournisseur F peut aussi organiser une loterie à laquelle participent ses clients qui utilisent le procédé selon l'invention pour faire des transactions avec lui. Par exemple, le serveur S est apte à

tirer aléatoirement le nom d'un gagnant parmi les clients connectés au serveur S à une heure donnée et à adresser au client gagnant une offre de cadeau.

De préférence, le serveur S est apte à mémoriser l'historique des transactions effectuées par un client donné à l'aide du procédé selon l'invention, par exemple le montant et la nature des transactions passées, et d'adapter les offres contenues dans les données de réponse 10 en fonction de la fidélité dudit client. Dans une variante de l'invention, les données de préférence 8 mémorisées dans la carte à puce P sont actualisées automatiquement en fonction des transactions effectuées par le client C à l'aide de ladite carte à puce P. L'historique des transactions passées du client C peut être mémorisé dans ladite unité de mémoire 1 et être inclus dans les données de préférence 8 communiquées au serveur S.

L'étape suivante du procédé est une étape de commande. Lorsque le client C a fait le choix d'un bien à commander au fournisseur F, il envoie au terminal T un ordre de commande 11 à l'aide de l'interface de commande 5. Par exemple, l'ordre de commande 11 est envoyé par simple actionnement d'un bouton de souris. Le terminal T demande alors la saisie du code d'identification personnel 9, pour vérifier que l'utilisateur de la carte à puce P est légitime. Lorsque le code saisi sur l'interface de commande 5 est conforme au code d'identification personnel 9 mémorisé dans l'unité de mémoire 1, le terminal T envoie automatiquement au serveur S des données de commande 146 et des données de paiement 120 chiffrées selon le premier code de chiffrement, les données de paiement 120 comportant toutes ou une partie des données personnelles 6 et des données bancaires 7, pour effectuer le paiement du bien.

Les données de commande 146 désignent un bien numérique 26 à fournir par le fournisseur F et disponible par l'intermédiaire du serveur S, c'est-à-dire, dans le mode de réalisation représenté, mémorisé sur le serveur S. Le bien numérique 26 est constitué d'un ensemble de données numériques utilisables, exécutables ou non. Avec le bien numérique 26, le client C choisit des modalités d'utilisation selon lesquelles il pourra utiliser le bien commandé. Par exemple, le prix du bien numérique commandé dépend des modalités

d'utilisation commandées avec celui-ci. Les données de commande 146 désignent donc également les modalités d'utilisation selon lesquelles ledit bien numérique est destiné à être utilisé.

A la réception des données de commande 146 et des données de paiement chiffrées 120, le serveur S procède à leur déchiffrement à l'aide de la première clé de déchiffrement 22. De préférence, le serveur S est apte à communiquer automatiquement avec un serveur informatique de vérification V, par exemple un serveur informatique d'un organisme bancaire, pour vérifier la validité des données bancaires 7 et/ou la solvabilité du client C. En réponse à la demande de vérification 15 envoyée par le serveur S, le serveur de vérification V envoie une confirmation de validité 16, positive ou négative selon que les données bancaires 7 sont jugées valides ou non. Lorsque la confirmation de validité 16 reçue est négative, le serveur S envoie au terminal T une commande d'annulation 17 pour annuler la transaction en cours. Dans des conditions particulières, pour prévenir une tentative d'achat illégitime, dans le cas, par exemple, où il n'existe pas de crédit identifié par les données bancaires 7, le serveur S envoie également une commande de blocage 18 pour bloquer la carte à puce P. Lorsque la confirmation de validité 16 reçue est positive, la commande est acceptée par le serveur S. Un compte de crédit du client est débité dans ce cas.

La fin de l'étape de commande va maintenant être décrite en référence à la figure 4. Le serveur S envoie au terminal T des données d'identification du bien commandé, chiffrées selon le second code de chiffrement. Sous la commande des moyens logiciels de pilotage 4, le terminal T redirige les données d'identification chiffrées vers la carte à puce P. Les données d'identification sont déchiffrées par le module de déchiffrement 13 de la carte à puce P et mémorisées dans l'unité de mémoire 1. Les données d'identification identifient de manière unique le bien commandé et payé par le client C, de manière à valoir pour preuves de la commande effectuée. Des modalités d'utilisation du bien, comme par exemple une durée maximale d'utilisation ou un nombre maximal d'utilisations sont comprises dans les données d'identification. Au sens de l'invention, les modalités d'utilisation incluent des données de droits d'utilisation 25.

Les données de droits d'utilisation 25 sont destinées à être lues dans le moyen électronique de paiement pour coopérer avec le bien numérique lorsqu'une utilisation du bien est ordonnée. Elles sont destinées à coopérer avec le bien numérique 26 pour autoriser son utilisation uniquement selon les modalités d'utilisation commandées par le client C, et en fonction desquelles le bien numérique est facturé.

Le bien numérique 26 comporte les données de droits d'utilisation 25, sous la forme d'un fichier de données séparé, et au moins un autre fichier informatique. Le bien numérique 26 peut être un programme d'ordinateur exécutable comme un logiciel de jeux vidéo, un logiciel éducatif ou une autre application commerciale. Un tel programme comporte par exemple un fichier exécutable permettant le démarrage du logiciel et des bibliothèques de fonctions, statiques ou dynamiques, qui sont appelées ou non par le fichier exécutable du logiciel en fonction des fonctionnalités utilisées par l'utilisateur. Ce programme d'ordinateur est conçu de manière que son exécution est impossible en l'absence des données de droits d'utilisation 25.

Les modalités d'utilisation commandées par le client C avec le programme d'ordinateur peuvent être des modalités chronologiques, comme une date limite d'exécution ou une durée totale d'exécution, limitée ou non ; des modalités quantitatives, comme un nombre total d'exécutions, limité ou non ; ou des modalités qualitatives comme un ensemble de fonctionnalités accessibles et utilisables, restreint ou non par rapport aux fonctionnalités complètes du programme d'ordinateur. Par exemple, dans un logiciel de jeux vidéo ou un logiciel éducatif comportant plusieurs niveaux successifs, le client C peut commander l'utilisation de certains niveaux seulement. Dans ce cas, les bibliothèques de fonctions correspondant aux niveaux dont l'utilisation n'a pas été commandée et payée sont fournies par le serveur S sous une forme verrouillée ou ne sont pas fournies.

Le bien numérique 26 peut aussi comporter un fichier de document non exécutable et utilisable par traitement au moyen d'un moyen de traitement approprié 29. Par exemple, il s'agit d'un fichier de document sonore, comme un disque numérisé au format MP3, d'un fichier de document audiovisuel, comme un film numérisé au format MPEG4, AVI, WAV ou MOV, d'un fichier de document graphique

comme une image au format JPG, GIF, ou d'un autre fichier de document comportant un contenu dans un format lisible par un logiciel de lecture approprié. Ce fichier de document est conçu de manière que son traitement est impossible en l'absence des données de droits d'utilisation 25.

Les modalités d'utilisation commandées par le client C avec le fichier de document peuvent être des modalités chronologiques, comme une date limite de lecture ou une durée totale de lecture, limitée ou non ; des modalités quantitatives, comme un nombre total de lectures, limité ou non ; ou des modalités qualitatives comme une restriction de lecture à une sous partie du fichier de document complet.

Comme identification du bien numérique 26, les données 25 comprennent par exemple le nom et le numéro de série du logiciel ou du document, sa date de création et la liste des fichiers qui en font partie.

Dans tous les cas, le serveur S envoie également au terminal T chaque fichier du bien numérique 26. Le bien numérique 26 est envoyé sous la forme des données de droits d'utilisation chiffrées 225, et du ou des autre(s) fichier(s) informatique(s) composé(s) d'une partie 226b chiffrée selon le second code de chiffrement et d'une partie non chiffrée 26a. La partie non chiffrée 26a ou la partie chiffrée 226b peut être vide. De préférence, la partie chiffrée 226b du ou des fichier(s) est aussi indispensable à l'utilisation du bien numérique 26. Par exemple, dans le cas où le bien est un programme d'ordinateur, une partie du code exécutable ou une des bibliothèques principales est contenue dans la partie 226b. Par exemple, dans le cas où le bien est un fichier de document audiovisuel, une tranche d'une demie seconde du document toutes les secondes est contenue dans la partie 226b.

A leur réception par le terminal T, la partie chiffrée 226b et la partie non chiffrée 26a du ou des autre(s) fichier(s) informatique(s) sont mémorisées dans une mémoire 27 du terminal T. Pour que le bien puisse être utilisé depuis le terminal T après téléchargement, par exemple pour écouter le disque acheté ou exécuter ledit logiciel acheté, la partie chiffrée 226b des fichiers doit être déchiffrée par le module cryptographique 13, puis retransmise au terminal T par la carte à puce P, comme représenté par la double

flèche 28 à la figure 4. Comme il va être maintenant expliqué en référence aux figures 5 et 6, les données de droits d'utilisation 25 (ou d'identification) sont destinées à être lues dans la carte à puce P lors de chaque utilisation du bien numérique 26 téléchargé. Ainsi, pour que le(s) fichier(s) du bien 26 puisse(nt) être utilisé(s), la carte à puce P qui a servi à passer la commande doit être connectée au lecteur 3.

On décrit maintenant, en référence à la figure 5, le déroulement d'une utilisation du bien numérique 26 téléchargé dans le cas où il s'agit d'un logiciel à plusieurs niveaux. A l'étape 30, un utilisateur donne, à travers l'interface de commande 5, un ordre d'exécution du logiciel. L'exécution du logiciel commence par l'étape 31, non soumise à autorisation, dans laquelle les données de droits d'utilisation 25 sont lues dans la mémoire 1, comme indiqué par la flèche 25 à la figure 4. Si la carte à puce P n'est pas connectée au lecteur 3, l'étape 31 n'est pas effectuée mais un message est adressé à l'utilisateur, par exemple : « veuillez introduire la carte dans le lecteur. »

A l'étape 32, le logiciel effectue une vérification des droits d'utilisation pour établir si l'exécution du logiciel est autorisée. Par exemple, la date limite d'exécution est comparée à la date actuelle donnée par l'horloge interne du terminal T ou la valeur d'un compteur d'exécutions est comparée à la valeur du nombre maximal d'exécutions autorisées contenu dans les droits d'utilisation 25. S'il est établi que l'utilisation n'est pas autorisée, par exemple la date limite d'exécution étant dépassée ou le nombre maximal d'exécutions ayant été atteint lors de l'exécution précédente, l'exécution est interrompue à l'étape 33.

Si l'exécution est autorisée, elle se poursuit à l'étape 34. La partie 226b du logiciel est alors complètement déchiffrée par le module 13 puis mémorisée déchiffrée dans la mémoire 27, de manière à pouvoir être exécutée ou appelée. Au cours de l'exécution du logiciel, l'utilisateur atteint la fin d'un niveau et demande l'accès au niveau supérieur à l'étape 35. Alors, à l'étape 36, les données de droits d'utilisation 25 sont au nouveau lues dans la mémoire 1, pour établir, à l'étape 37, si l'accès au niveau supérieur est autorisé, par exemple en comparant le numéro dudit niveau supérieur à une liste des niveaux accessibles contenue dans les données 25. S'il est établi que l'accès au

niveau supérieur n'est pas autorisée, l'exécution de ce niveau est refusée à l'étape 38 et un message « niveau non accessible » est affiché à l'écran. Si l'accès est autorisé, le niveau supérieur est exécuté à l'étape 39.

En variante, la partie chiffrée 226b n'est que partiellement déchiffrée à l'étape 34, des fonctions non nécessaires à l'exécution du niveau courant restant chiffrée pour être déchiffrée ultérieurement, lorsqu'elle seront nécessaires à la poursuite de l'exécution. Par exemple, les fonctions nécessaires à l'exécution du niveau supérieur sont déchiffrées lors du passage au niveau supérieur lorsque ce passage est autorisé.

On décrit maintenant, en référence à la figure 6, le déroulement d'une utilisation du bien numérique 26 téléchargé dans le cas où il s'agit d'un fichier de document, par exemple d'une séquence musicale numérisée. A l'étape 40, un utilisateur donne, à travers l'interface de commande 5, un ordre de lecture de la séquence musicale, par exemple en cliquant sur une icône correspondante. A l'étape 41 est lancée la mise en œuvre d'un moyen de traitement 29, visible à la figure 4, à savoir, dans le présent exemple, l'exécution d'un logiciel de lecture 29 apte à lire le format de numérisation employé dans le bien numérique 26. L'exécution du logiciel de lecture commence par l'étape 42, non soumise à autorisation, dans laquelle les données de droits d'utilisation 25 sont lues dans la mémoire 1, comme indiqué par la flèche 25 à la figure 4. Si la carte à puce P n'est pas connectée au lecteur 3, l'étape 31 n'est pas effectuée mais un message est adressé à l'utilisateur, par exemple : « veuillez introduire la carte dans le lecteur. »

A l'étape 43, le logiciel effectue une vérification des droits d'utilisation pour établir si la lecture du fichier de document est autorisée. Par exemple, la date limite de lecture est comparée à la date actuelle donnée par l'horloge interne du terminal T ou la valeur d'un compteur de lectures est comparée à la valeur du nombre maximal de lectures autorisées contenu dans les droits d'utilisation 25. S'il est établi que la lecture n'est pas autorisée, l'exécution du logiciel de lecture est interrompue à l'étape 44.

Si la lecture est autorisée, elle se produit à l'étape 45. La partie 226b du fichier de document est alors déchiffrée par le module 13, soit entièrement avant le démarrage de la lecture proprement dite, soit en temps réel à mesure que les parties chiffrées sont atteintes au cours de la lecture du document.

Le traitement par le moyen de traitement 29 du fichier de document produit les effets attendus par l'utilisateur, à savoir, dans le présent exemple, l'émission de la séquence musicale par un équipement de reproduction sonore, non représenté, relié au terminal T. Le moyen de traitement 29 peut être installé sur le terminal T avant l'acquisition du bien numérique 26. En variante, lorsqu'il s'agit d'un logiciel exécutable, le moyen de traitement 29 peut être fourni depuis le serveur S dans le conditions précitées. Par exemple, le bien numérique 26 comprend un fichier de document et un logiciel de lecture correspondant, chacun ou l'un d'eux ayant ses modalités d'utilisation prédéfinies par les données 25.

Lorsqu'un utilisateur souhaite élargir ou renouveler ses droits d'utilisation d'un bien numérique acquis précédemment, par exemple pour accéder à un niveau du logiciel auquel il n'avait pas acquis l'accès, ou pour acquérir le droits à des lectures supplémentaire s du fichier de document après épuisement du nombre maximal de lectures autorisées qu'il avait acquis initialement, il peut commander à l'aide du dispositif selon l'invention des droits d'utilisation seuls, de manière à renouveler les données de droits d'utilisation 25 mémorisées sur sa carte à puce. Il n'a pas besoin de télécharger à nouveau les autres fichiers informatiques déjà mémorisés sur le terminal d'achat pour les utiliser à nouveau.

Bien que l'invention ait été décrite en liaison avec plusieurs variantes de réalisation particulières, il est bien évident qu'elle n'y est nullement limitée et qu'elle comprend tous les équivalents techniques des moyens décrits ainsi que leurs combinaisons, si celles-ci entrent dans le cadre de l'invention.

REVENDICATIONS

1. Procédé de distribution commerciale en ligne de biens numériques par l'intermédiaire d'un réseau de communication (R), ledit procédé comprenant les étapes consistant à :

(a) mettre en communication de manière amovible avec un premier terminal informatique (T), dit terminal d'achat, un moyen électronique de paiement (P) destiné à être porté par un client (C), des données de crédit (7) identifiant un crédit dudit client étant mémorisées dans une mémoire (1) dudit moyen électronique de paiement,

(b) à la suite d'un ordre de commande (11) donné par ledit client au terminal d'achat pour commander un bien numérique de son choix, envoyer lesdites données de crédit (7) depuis le terminal d'achat (T) à destination d'un second terminal informatique (S), dit serveur, d'un fournisseur (F), lesdites données de crédit étant chiffrées, ledit serveur et ledit terminal d'achat étant aptes à communiquer par l'intermédiaire dudit réseau de communication (R),

(c) vérifier la validité desdites données de crédit et, lorsque lesdites données de crédit sont valides,

(d) envoyer, depuis le serveur à destination du terminal d'achat, ledit bien numérique (26) comprenant au moins un fichier de données numériques exécutable ou non ,

caractérisé par le fait que ledit bien numérique comprend un fichier séparé de données de droits d'utilisation (225) définissant des modalités d'utilisation du bien numérique choisies par le client et un ou plusieurs autre(s) fichier(s) de données, lesdites données de droits d'utilisation étant envoyées chiffrées selon un code de chiffrement pour lequel une clé de déchiffrement secrète (12) est mémorisée dans la mémoire (1) dudit moyen électronique de paiement (P), ledit procédé comportant les étapes consistant à :

(e) mémoriser le ou lesdits autres fichier(s) de données (26a, 226b) sur le terminal d'achat,

(f) mémoriser dans ladite mémoire (1) du moyen électronique de paiement (P) lesdites données de droits d'utilisation (25) en les déchiffrant à l'aide de ladite clé de déchiffrement (12), lesdites données de droits d'utilisation étant indispensables à l'utilisation dudit bien numérique.

2. Procédé selon la revendication 1, caractérisé par le fait que ledit ordre de commande (11) produit l'envoi par le terminal d'achat, à destination du serveur, de données de commandes (146) désignant ledit bien numérique choisi par le client et les modalités d'utilisation choisies par le client, selon lesquelles ledit bien numérique est destiné à être utilisé, les données de droits d'utilisation étant destinées à autoriser une utilisation dudit bien numérique selon lesdites modalités d'utilisation choisies.

3. Procédé selon la revendication 1 ou 2, caractérisé par le fait que ledit ou lesdits autres fichier(s) comprend/comprennent un programme d'ordinateur exécutable, ladite utilisation comportant une exécution dudit programme d'ordinateur, ledit programme d'ordinateur étant conçu de manière que son exécution comporte des opérations (31) non soumises à autorisation consistant à lire les données de droits d'utilisation (25) dans ledit moyen électronique de paiement (P) et à autoriser ou non (32), en fonction desdites données de droits d'utilisation, l'exécution d'au moins une opération suivante (34) soumise à autorisation.

4. Procédé selon la revendication 1 ou 2, caractérisé par le fait que ledit ou lesdits autres fichier(s) comprend/comprennent au moins un fichier de document non exécutable, ladite utilisation comportant des opérations non soumises à autorisation consistant à lire (42) les données de droits d'utilisation (25) dans ledit moyen électronique de paiement (P) et à autoriser ou non (43), en fonction desdites données de droits d'utilisation, l'exécution d'au moins une opération (45) de traitement dudit ou desdits fichier(s) de document par un moyen de traitement correspondant (29).

5. Procédé selon les revendications 3 et 4 prises en combinaison, caractérisé par le fait que ledit programme d'ordinateur exécutable par ledit terminal d'achat constitue ledit moyen de traitement (29), ladite ou lesdites opération(s) suivante(s) comportant ladite ou lesdites opération(s) (45) de traitement dudit ou desdits fichier(s) de document.

6. Procédé selon l'une des revendications 1 à 5, caractérisé par le fait qu'il comporte une étape consistant à :

(i) chiffrer au moins partiellement ledit ou lesdits autre(s) fichier(s) de

données selon ledit code de chiffrement avant de le(s) mémoriser sur le terminal d'achat, ledit procédé comportant une étape de déchiffrement (28) de la partie chiffrée (226b) dudit ou desdits autre(s) fichier(s) de données par ledit moyen électronique de paiement (P) lorsqu'une utilisation du bien numérique est ordonnée (30, 40).

7. Procédé selon l'une des revendications 1 à 6, caractérisé par le fait qu'il comporte, avant l'étape (a), une étape consistant à fournir au client le moyen électronique de paiement avec des clés de chiffrement (19) et de déchiffrement (12) incluses et pour lesquelles clés le fournisseur possède des clés de déchiffrement (22) et de chiffrement (23) respectives correspondantes.

8. Procédé selon l'une des revendications 1 à 7, caractérisé par le fait que les modalités d'utilisation définies par lesdites données de droits d'utilisation (25) comportent des modalités chronologiques comme une durée maximale d'utilisation ou une date limite d'utilisation, et/ou des modalités quantitatives comme un nombre maximal d'utilisations, et/ou des modalités qualitatives comme une restriction de l'utilisation à un sous-ensemble dudit bien numérique.

9. Dispositif électronique pour acheter des biens numériques en ligne par l'intermédiaire d'un réseau de communication (R), ledit dispositif comprenant :

- un moyen électronique de paiement (P) destiné à être porté par un client (C) et muni d'une mémoire (1), des données de crédit (7) identifiant un crédit dudit client (C) étant mémorisées dans ladite mémoire (1),
- un terminal informatique d'achat (T) relié à un serveur informatique (S) dudit fournisseur (F) par ledit réseau de communication (R), et muni d'une interface de commande (5) pour recevoir un ordre de commande (11) donné par le client pour commander un bien numérique de son choix,
- une interface électronique (3) reliée audit terminal d'achat (T), ladite interface électronique étant apte à recevoir de manière amovible ledit moyen électronique de paiement (P) pour permettre un échange de données entre ledit terminal d'achat (T) et ledit moyen électronique de paiement (P),
- des moyens logiciels de pilotage (4) pour piloter les opérations

consistant à :

(a) envoyer lesdites données de crédit (7) depuis ledit moyen électronique de paiement à destination dudit serveur (S), lesdites données de crédit étant chiffrées,

(b) lorsque lesdites données de crédit ont été validées, recevoir depuis le serveur ledit bien numérique (26) comprenant au moins un fichier de données exécutable ou non,

caractérisé par le fait que ledit bien numérique comprend un fichier séparé de données de droits d'utilisation (225) définissant des modalités d'utilisation du bien numérique choisies par le client et un ou plusieurs autre(s) fichier(s) de données, lesdites données de droits d'utilisation étant reçues chiffrées, lesdits moyens logiciels de pilotage (4) étant aptes à piloter les opérations consistant à :

(c) mémoriser ledit ou lesdits autres fichier(s) de données (26a, 226b) sur le terminal d'achat,

(d) mémoriser lesdites données de droits d'utilisation (225, 25) dans ladite mémoire (1) du moyen électronique de paiement (P) en les faisant déchiffrer par le moyen électronique de paiement à l'aide d'une clé de déchiffrement secrète (12) mémorisée dans la mémoire (1), lesdites données de droits d'utilisation étant indispensables à l'utilisation dudit bien numérique.

10. Dispositif électronique selon la revendication 9, caractérisé par le fait que ladite interface de commande (5) permet au client d'ordonner (30, 40) une utilisation dudit bien numérique.

11. Dispositif électronique selon la revendication 10, caractérisé par le fait que ledit ou lesdits autre(s) fichier(s) de données est/sont reçu(s) au moins partiellement chiffré(s) selon ledit code de chiffrement, lesdits moyens logiciels de pilotage (4) étant aptes à piloter une opération (28) consistant à faire déchiffrer la partie chiffrée (226b) dudit ou desdits autre(s) fichier(s) de données par le moyen électronique de paiement à l'aide de ladite clé de déchiffrement secrète (12) lorsque ladite utilisation est ordonnée.

12. Système d'achat en ligne prêt à installer comportant ledit moyen électronique de paiement (P), ladite interface électronique (3) et lesdits moyens logiciels de pilotage (4) du dispositif électronique selon l'une des revendications 9 à 11, ledit moyen électronique de

paiement étant ou non relié à ladite interface électronique, ladite interface électronique étant ou non reliée audit terminal d'achat et lesdits moyens logiciels étant fixés sur un support de données.

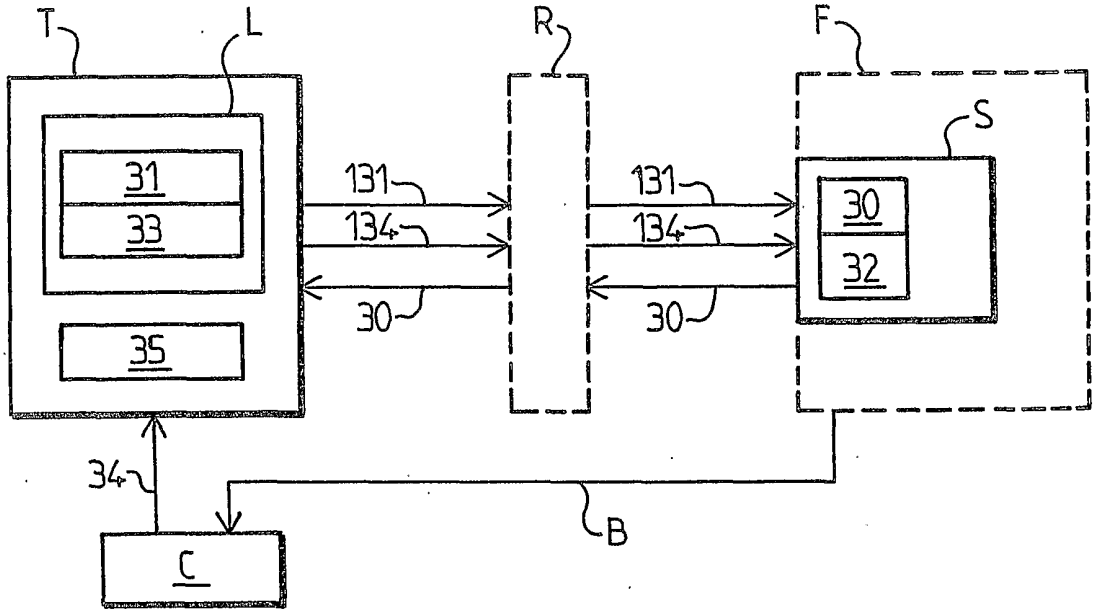


FIG.1 ART ANTERIEUR

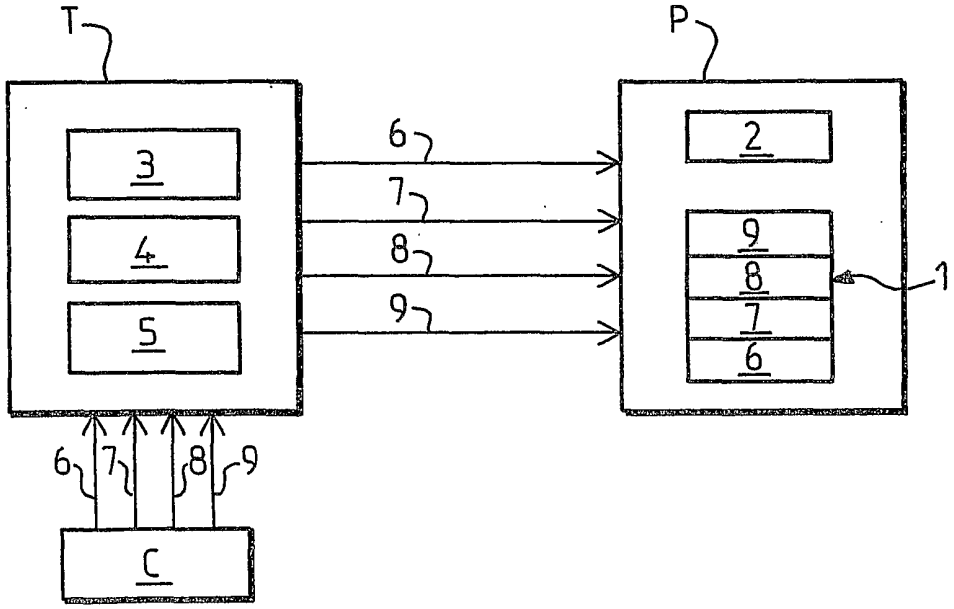


FIG.2

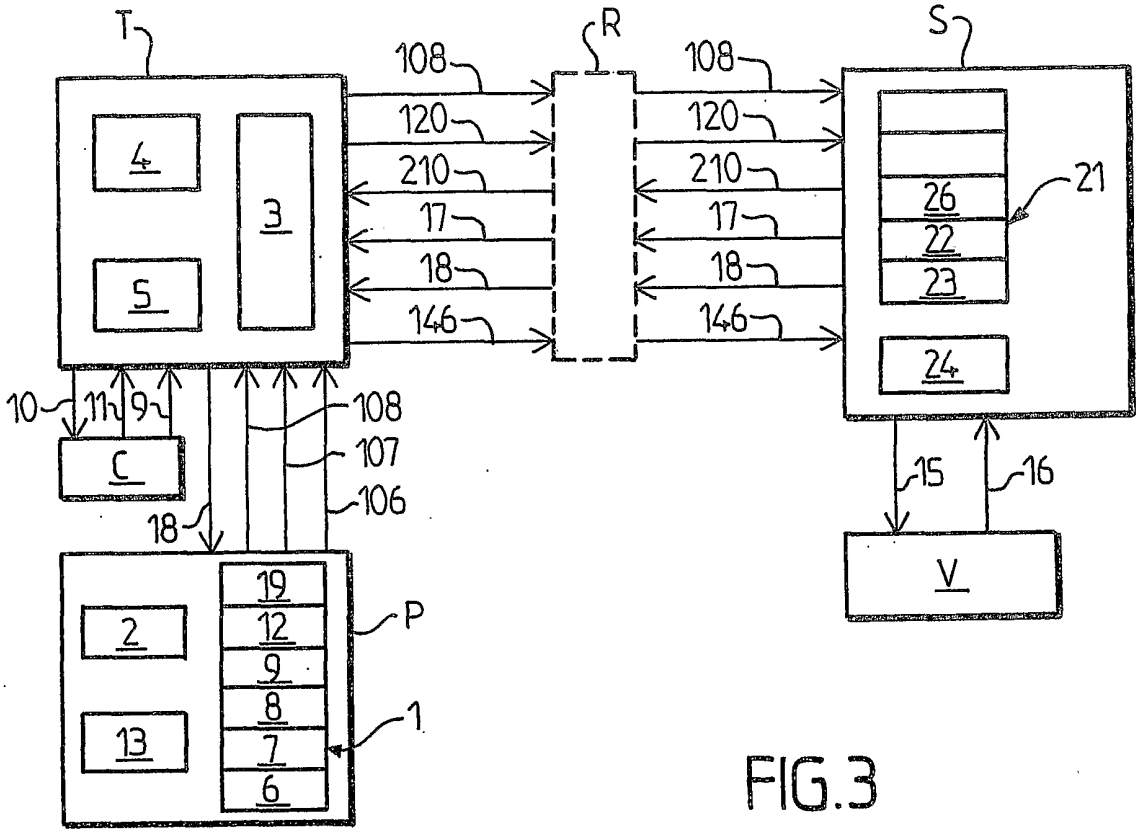

T
R
S
108
120
210
17
18
146
4
3
5
26
22
23
21
24
10
11
9
C
107
106
15
16
V
2
13
19
12
9
8
7
6
P
1

FIG.3

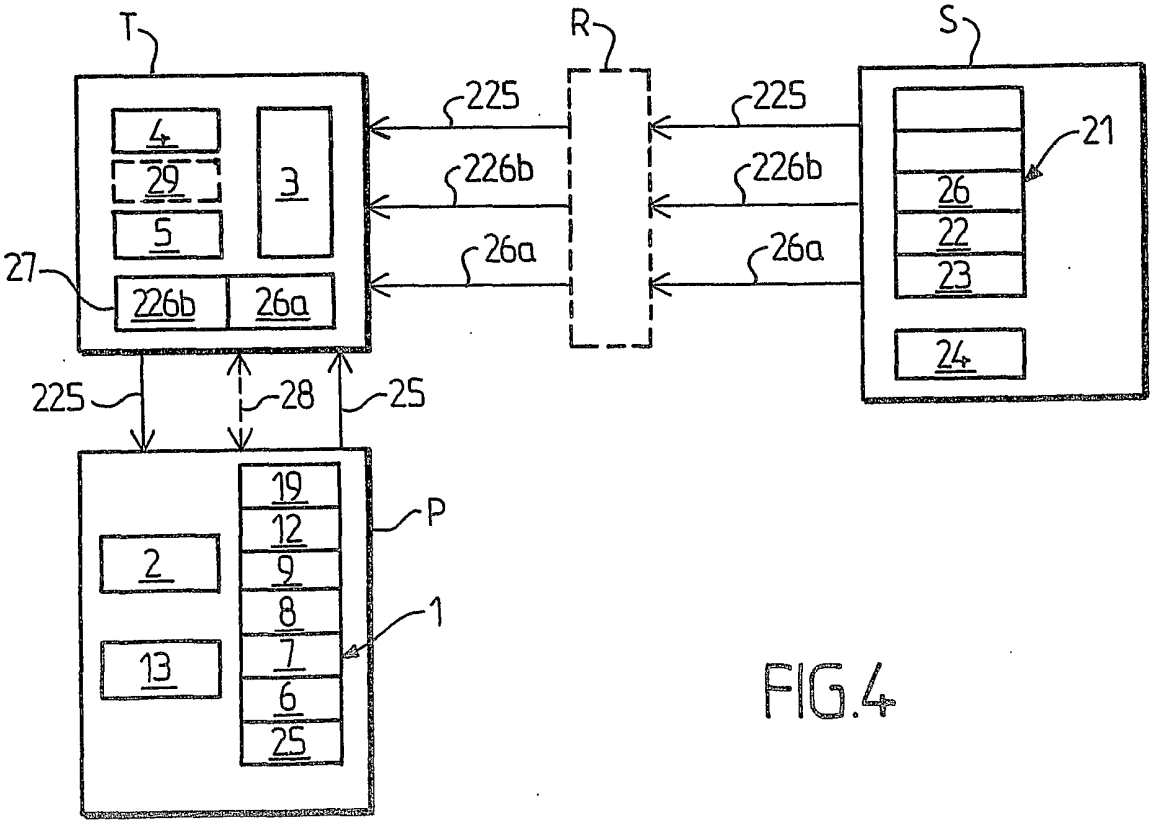

T
R
S
225
226b
26a
4
29
3
5
27
226b
26a
21
26
22
23
24
225
28
25
19
12
9
8
7
6
25
P
2
13
1

FIG.4

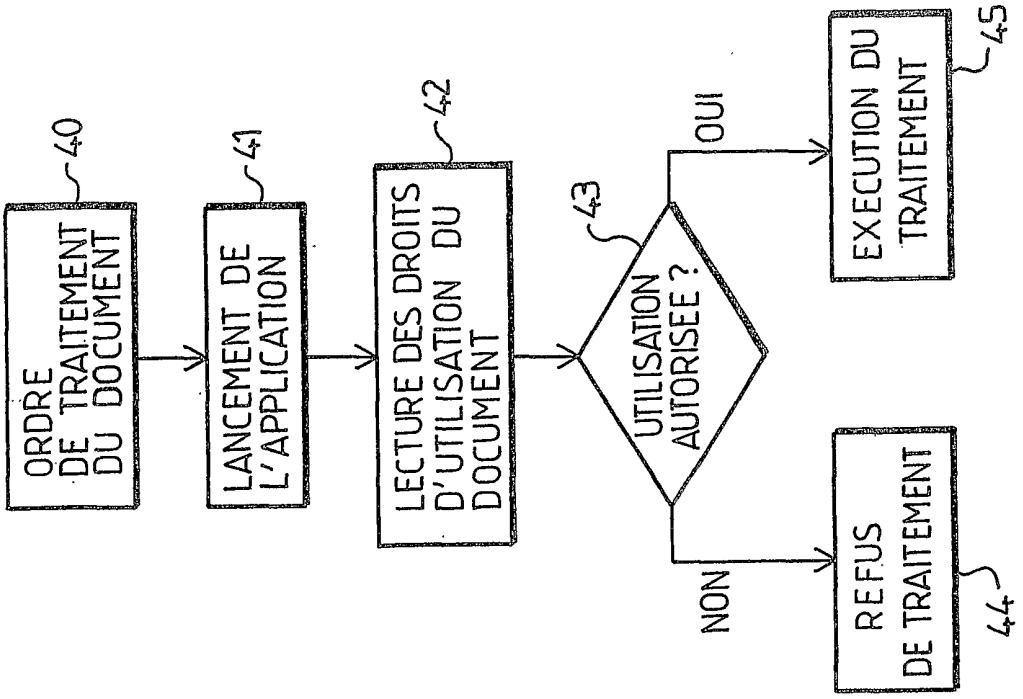

ORDRE DE TRAITEMENT DU DOCUMENT
40
LANCEMENT DE L'APPLICATION
41
LECTURE DES DROITS D'UTILISATION DU DOCUMENT
42
UTILISATION AUTORISEE ?
43
OUI
EXECUTION DU TRAITEMENT
45
NON
REFUS DE TRAITEMENT
44

FIG.6

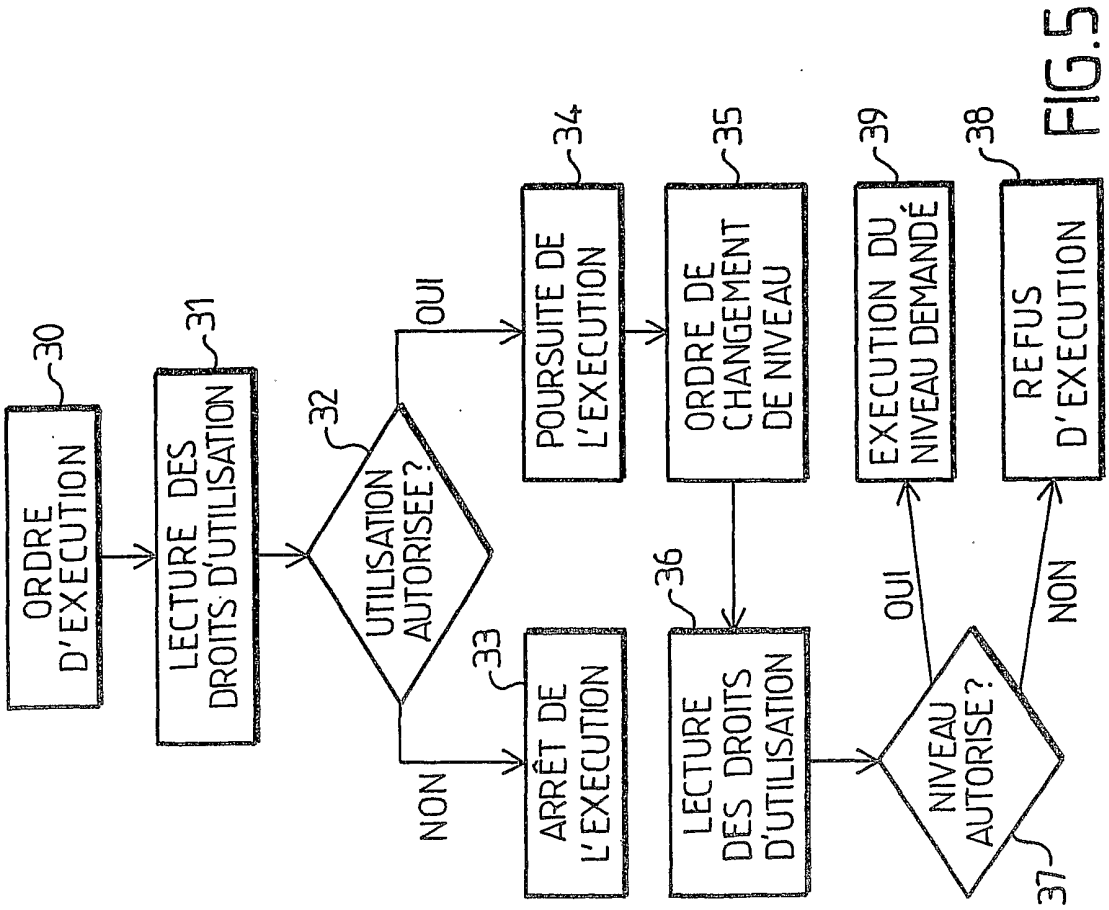

ORDRE D'EXECUTION
30
LECTURE DES DROITS D'UTILISATION
31
UTILISATION AUTORISEE ?
32
OUI
POURSUITE DE L'EXECUTION
34
ORDRE DE CHANGEMENT DE NIVEAU
35
EXECUTION DU NIVEAU DEMANDÉ
39
REFUS D'EXECUTION
38
NON
ARRÊT DE L'EXECUTION
33
LECTURE DES DROITS D'UTILISATION
36
NIVEAU AUTORISE ?
37
OUI
NON

FIG.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02013

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60

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 G06F

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, INSPEC, IBM-TDB, PAJ, WPI Data, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 49615 A (MICROTOME INC ;SAIGH MICHAEL M (US)) 30 September 1999 (1999-09-30) page 2, line 15 -page 4, line 3 page 11, line 6 - line 17 page 14, line 17 -page 15, line 18 page 16, line 11 -page 20, line 2 page 26, line 12 -page 30, line 15 figures 2,3	1-12
X	EP 0 917 119 A (CITICORP DEV CENTER INC) 19 May 1999 (1999-05-19) column 18, line 30 -column 20, line 36	1-12

-/--

[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
28 August 2001	04/09/2001

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	Marcu, A

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

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02013

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	HAMANN U.: "Chip cards-the application revolution" ELECTRON DEVICES MEETING, 1997. TECHNICAL DIGEST., INTERNATIONAL, 'Online! 7 - 10 December 1997, pages 15-22, XP002166812 ISBN: 0-7803-4100-7 Retrieved from the Internet: <URL:http://ieeexplore.ieee.org> 'retrieved on 2001-05-08! page 15 -page 22 ---	1-12
A	US 5 809 144 A (TYGAR J D ET AL) 15 September 1998 (1998-09-15) page 1, line 62 -page 2, line 62 column 3, line 56 -column 4, line 16 -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/02013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9949615 A	30-09-1999	AU 1109499 A	18-10-1999
		CN 1292960 T	25-04-2001
		EP 1074113 A	07-02-2001
EP 0917119 A	19-05-1999	AU 1584499 A	31-05-1999
		AU 1796599 A	31-05-1999
		AU 9234698 A	03-06-1999
		BR 9806416 A	16-11-1999
		CN 1233804 A	03-11-1999
		EP 0917120 A	19-05-1999
		EP 0950972 A	20-10-1999
		JP 11250165 A	17-09-1999
		JP 11232348 A	27-08-1999
		SG 78323 A	20-02-2001
		TW 381241 B	01-02-2000
		WO 9924891 A	20-05-1999
		WO 9924892 A	20-05-1999
		US 2001011250 A	02-08-2001
		EP 0951158 A	20-10-1999
		EP 0950992 A	20-10-1999
		JP 2000036049 A	02-02-2000
		JP 2000076189 A	14-03-2000
		JP 2000251006 A	14-09-2000
		SG 76609 A	21-11-2000
US 5809144 A	15-09-1998	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/02013

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F17/60

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 G06F

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, INSPEC, IBM-TDB, PAJ, WPI Data, COMPENDEX

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 99 49615 A (MICROTOME INC ;SAIGH MICHAEL M (US)) 30 septembre 1999 (1999-09-30) page 2, ligne 15 -page 4, ligne 3 page 11, ligne 6 - ligne 17 page 14, ligne 17 -page 15, ligne 18 page 16, ligne 11 -page 20, ligne 2 page 26, ligne 12 -page 30, ligne 15 figures 2,3	1-12
X	EP 0 917 119 A (CITICORP DEV CENTER INC) 19 mai 1999 (1999-05-19) colonne 18, ligne 30 -colonne 20, ligne 36	1-12

-/--

[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'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
28 août 2001	04/09/2001

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	Marcu, A

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/02013

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	HAMANN U.: "Chip cards-the application revolution" ELECTRON DEVICES MEETING, 1997. TECHNICAL DIGEST., INTERNATIONAL, 'en ligne! 7 - 10 décembre 1997, pages 15-22, XP002166812 ISBN: 0-7803-4100-7 Extrait de l'Internet: <URL:http://ieeexplore.ieee.org> 'extrait le 2001-05-08! page 15 -page 22 ---	1-12
A	US 5 809 144 A (TYGAR J D ET AL) 15 septembre 1998 (1998-09-15) page 1, ligne 62 -page 2, ligne 62 colonne 3, ligne 56 -colonne 4, ligne 16 -----	1-12

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/02013

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9949615 A	30-09-1999	AU 1109499 A	18-10-1999
		CN 1292960 T	25-04-2001
		EP 1074113 A	07-02-2001
EP 0917119 A	19-05-1999	AU 1584499 A	31-05-1999
		AU 1796599 A	31-05-1999
		AU 9234698 A	03-06-1999
		BR 9806416 A	16-11-1999
		CN 1233804 A	03-11-1999
		EP 0917120 A	19-05-1999
		EP 0950972 A	20-10-1999
		JP 11250165 A	17-09-1999
		JP 11232348 A	27-08-1999
		SG 78323 A	20-02-2001
		TW 381241 B	01-02-2000
		WO 9924891 A	20-05-1999
		WO 9924892 A	20-05-1999
		US 2001011250 A	02-08-2001
		EP 0951158 A	20-10-1999
		EP 0950992 A	20-10-1999
		JP 2000036049 A	02-02-2000
		JP 2000076189 A	14-03-2000
		JP 2000251006 A	14-09-2000
		SG 76609 A	21-11-2000
US 5809144 A	15-09-1998	AUCUN	