(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 797 974**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 12108**

(51) Int Cl[7] : **G 06 F 19/00**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.09.99.

(30) **Priorité :** 30.08.99 FR 09911250.

(43) **Date de mise à la disposition du public de la demande :** 02.03.01 Bulletin 01/09.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CORNUEJOLS GEORGES MARC* — FR.

(72) **Inventeur(s) :** CORNUEJOLS GEORGES MARC.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CORNUEJOLS GEORGES.

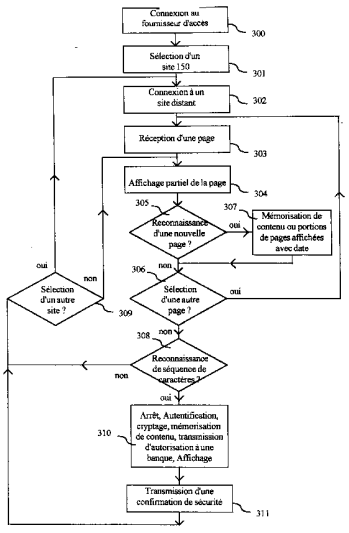
(54) PROCEDE ET DISPOSITIF DE SECURITE DE PAIEMENT.

(57) Le procédé de sécurisation comporte une opération d'ouverture d'une session de communication entre un terminal informatique et un site informatique, par l'intermédiaire d'un réseau de communication.

Ce procédé comporte aussi une opération de détection automatique de préparation d'un paiement par l'intermédiaire du terminal.

Enfin, lorsqu'une préparation de paiement est détectée, une opération automatique de sécurisation dudit paiement est automatiquement effectuée en sauvegardant au moins le montant du paiement en dehors dudit site informatique.

Préférentiellement, l'opération de détection est effectuée en tâche de fond par rapport à la session de communication, l'opération de préparation de paiement.



FR 2 797 974 - A1

2797974

La présente invention concerne un procédé et un dispositif de sécurité. Plus particulièrement, la présente invention s'applique à sécuriser des données, des communications ou des transactions en ligne. Encore plus particulièrement, la présente invention s'attache à sécuriser des paiements effectués par l'intermédiaire d'un réseau de communication, par exemple l'Internet.

Lorsque l'on accède à des données, localement ou à distance, on ne conserve trace de leur contenu ou de l'accès effectué que selon des méthodes laborieuses de mémorisation page par page. Lorsque l'on paye en ligne, on ne dispose pas de trace du paiement. Lorsque l'on paye en ligne, on doit généralement saisir toute une série de chiffres (par exemple 16) qui identifient un moyen de paiement (par exemple une carte de paiement). Cette opération est laborieuse et présente d'importants risques d'erreur.

Lorsque l'on effectue une transaction avec un fournisseur par l'intermédiaire d'un réseau de communication, on n'a généralement aucune autre trace de la transaction effectuée que l'éventuelle confirmation effectuée par le fournisseur. De plus, la transaction ne présente alors que le niveau de sécurité financière, technique ou juridique « offert » par le fournisseur.

Ayant identifié chacun de ces problèmes, l'inventeur vise, à travers la présente invention et selon certains de ses aspects, à résoudre ces problèmes.

Selon un premier aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte :

- une opération d'ouverture de communication avec un site informatique distant,
- une opération de détection automatique de données relatives à un paiement et
- à la suite d'une détection de dites données, une opération de protection de l'usage desdites données.

Selon un deuxième aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte une opération de sauvegarde de tout contenu au format « texte » reçu par un terminal par l'intermédiaire d'un réseau de communication.

Selon des caractéristiques particulières de ce deuxième aspect, l'opération de sauvegarde comporte une opération de proposition à l'utilisateur de sauvegarde pour chaque session de communication sur ledit réseau de communication.

Selon d'autres caractéristiques particulières de ce deuxième aspect, le contenu reçu au format texte est organisé dans une banque de données et au cours d'une opération de recherche, des mots clés sont recherchés dans les données au format texte reçues.

Selon un troisième aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte :

- une opération d'ouverture de communication par un utilisateur,
- une opération de détection automatique d'un engagement dudit utilisateur,
- à la suite d'une détection d'un dit engagement de l'utilisateur, une opération de limitation de risques lié audit engagement.

Selon un quatrième aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte une opération de détection d'un identifiant d'un moyen de paiement et une opération de sécurisation de l'usage desdits moyens de paiement.

Selon un cinquième aspect, la présente invention vise un procédé de transmission d'identifiant d'un moyen de paiement, caractérisé en ce qu'il comporte une sélection d'un icône par un utilisateur et dès sélection de cet icône une copie dudit identifiant.

Selon un sixième aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication entre un terminal informatique et un site informatique, par l'intermédiaire d'un réseau de communication,
- une opération de détection automatique d'une préparation de paiement par transmission, au cours de ladite session, par l'intermédiaire dudit terminal, d'un identifiant d'un moyen de paiement, et
- lorsqu'une préparation de paiement est détectée, une opération automatique de sécurisation dudit paiement en dehors dudit site informatique, ladite opération de sécurisation comportant au moins une opération de sauvegarde du montant du paiement en dehors dudit site informatique.

Selon des caractéristiques particulières, l'opération de détection de préparation d'un paiement comporte une opération de détection d'un identifiant d'un moyen de paiement. Grâce à ces dispositions, la détection est effectuée de manière simple, fiable et techniquement peut coûteuse en durée de développement, en capacité de calcul ou en capacité de mémoire, par une simple surveillance dudit identifiant.

Selon des caractéristiques particulières, le procédé comporte une opération de saisie de symboles par l'intermédiaire d'un clavier dudit terminal, et l'opération de détection comporte

une opération de reconnaissance, parmi les symboles saisis au cours de l'opération de saisie, de tout ou partie :

- d'un numéro de carte de paiement ou de crédit,
- d'une date de péremption d'une telle carte, et/ou
- d'un numéro de compte bancaire.

Grâce à ces dispositions, une simple surveillance, en tache de fond, des symboles saisis par l'utilisateur permet la détection de la préparation d'un paiement. Cette opération de détection est alors compatible avec tous les logiciels de communication ou de navigation sur réseau déjà existants et ne nécessitent pas leur adaptation.

Selon d'autres caractéristiques particulières, l'opération de reconnaissance comporte une opération de comparaison d'une succession de symboles saisis et d'au moins une séquence de symboles conservée en mémoire.

Grâce à ces dispositions, en mettant en mémoire une succession de quatre chiffres appartenant à un numéro de carte de crédit ou de paiement ou à un numéro de compte bancaire ou encore la date d'expiration de validité du moyen de paiement, on permet la détection automatique d'un paiement mettant en oeuvre ledit moyen de paiement.

Selon d'autres caractéristiques particulières, l'opération de reconnaissance comporte une opération de détection d'une succession de symboles saisis présentant une caractéristique prédéterminée.

Grâce à ces dispositions, l'utilisation d'une carte de paiement ou de crédit ou d'un numéro de compte en banque, peut être détectée par la longueur de son numéro et/ou par l'association d'un numéro et d'une date.

Selon d'autres caractéristiques particulières, l'opération de sécurisation comporte :

- une opération de mise en mémoire des données échangées avec un format « texte » au cours de la session,
- une opération de communication à un tiers de confiance, de données relatives au paiement,
- une opération d'affichage de données juridiques,
- une opération d'impression d'un détail des paiements déjà effectués en ligne, et/ou
- une opération de cryptage de la transmission de données confidentielles.

Grâce à chacune de ces dispositions, la sécurisation est de mise en oeuvre simple et efficace et garantit, techniquement, financièrement et/ou juridiquement l'utilisateur contre une utilisation abusive de son consentement contractuel et/ou de ses moyens de paiement.

Selon des caractéristiques particulières, l'opération de détection est effectuée en tâche de fond par rapport à la session de communication et l'opération de préparation de paiement. Grâce à ces dispositions, la mise en oeuvre du procédé est compatible avec tout logiciel et ne gêne pas l'utilisateur pendant la session de communication jusqu'à la préparation de paiement.

Selon un septième aspect, la présente invention vise un dispositif de sécurisation, caractérisé en ce qu'il comporte :

- un terminal informatique qui ouvre une session de communication avec un site informatique, par l'intermédiaire d'un réseau de communication,

- un moyen de détection automatique de préparation d'un paiement par l'intermédiaire du terminal, et

- un moyen de sécurisation dudit paiement, lorsqu'une préparation de paiement est détectée comportant un moyen de sauvegarde d'au moins un montant de paiement en dehors dudit site informatique.

On observe que le moyen de détection peut se trouver sur le réseau de communication, en tout endroit (à l'exception du site informatique), et, en particulier, dans le terminal informatique ou dans un système informatique d'un fournisseur d'accès audit réseau. On observe que le moyen de sécurisation peut aussi se trouver sur le réseau de communication, en tout endroit (à l'exception du site informatique) et, en particulier, dans le terminal informatique ou dans un système informatique d'un fournisseur d'accès audit réseau.

La présente invention vise aussi un site informatique, un serveur, un ordinateur, caractérisé en ce qu'ils mettent en oeuvre le procédé succinctement exposé ci-dessus. La présente invention vise aussi un support d'information, tel qu'une disquette, un disque dur, un compact disque ou une mémoire d'ordinateur, qui conserve des instructions de programme pour :

- ouvrir une session de communication entre un terminal informatique et un site informatique, par l'intermédiaire d'un réseau de communication,

- détecter automatiquement une préparation de paiement par transmission, au cours de ladite session, par l'intermédiaire dudit terminal, d'un identifiant d'un moyen de paiement, et

- lorsqu'une préparation de paiement est détectée, sécuriser automatiquement ledit paiement en dehors dudit site informatique, au moins en sauvegardant le montant du paiement en dehors dudit site informatique.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre, faite dans un but explicatif et nullement limitatif, en regard des dessins annexés dans lesquels :

- la figure 1 représente un mode de réalisation d'un dispositif adapté à la mise en oeuvre du procédé objet de la présente invention,

- la figure 2 représente un écran de visualisation au cours de la mise en oeuvre d'un premier mode de réalisation du procédé objet de la présente invention,

- la figure 3 représente un organigramme de fonctionnement du dispositif illustré en figure 1, selon le premier mode de réalisation du procédé objet de la présente invention,

- la figure 4 représente un organigramme de fonctionnement du dispositif illustré en figure 1, selon un deuxième mode de réalisation du procédé objet de la présente invention,

- la figure 5 représente un écran de visualisation au cours de la mise en oeuvre du deuxième mode de réalisation du procédé objet de la présente invention,

- la figure 6 représente un organigramme de fonctionnement de chacun des premier et deuxième modes de réalisation illustrés en figures 3 et 4, et

- la figure 7 représente un organigramme de fonctionnement d'un aspect particulier de la présente invention.

Selon l'un de ses aspects, illustré en figure 7, le procédé objet de la présente invention détecte automatiquement (opération 820), au cours d'une session de communication (ouverte au cours d'une opération 800) entre un terminal informatique d'un utilisateur et un site informatique, sur un réseau tel qu'Internet, que l'utilisateur prépare un paiement par transmission, au cours de la session et par l'intermédiaire de son terminal, d'un identifiant d'un moyen de paiement (opération 810). Par exemple, cette détection est effectuée en reconnaissant, parmi les chiffres saisis par l'intermédiaire d'un clavier du terminal, tout ou partie d'un numéro de carte de paiement ou de crédit (et/ou d'une date de péremption d'une telle carte, et/ou d'un numéro de compte bancaire et/ou d'une demande de certificat de transaction). Lorsque cette préparation de paiement est détectée, une opération 830 de sécurisation dudit paiement.

Cette opération 830 de sécurisation (soit, par exemple, de protection contre un usage abusif du consentement de l'utilisateur lié audit paiement) comporte au moins une opération 837 de sauvegarde, en dehors du site informatique distant, du montant du paiement. L'opération de sauvegarde peut être effectuée en mémorisant ce montant, en l'imprimant ou en le transmettant à distance. L'opération 830 peut comporter, en outre, par exemple, une

authentification de l'utilisateur 831, une mise en mémoire des données échangées avec un format « texte » au cours de la session 832, une communication à un tiers de confiance, tel qu'une banque auprès de laquelle le paiement doit être effectué, de données relatives au paiement (montant, fournisseur) 833, un affichage de données juridiques 834, l'impression d'informations relatives à la transaction ou d'un détail des paiements déjà effectués en ligne 835, un cryptage de la transmission de données confidentielles 836, un affichage de questionnaire en vue de son renseignement 838.

Ceci permet à l'utilisateur d'avoir au moins une protection juridique car une trace de l'accord contractuel existe, et une protection financière car le paiement est limité au montant convenu.

Pour chacun des aspects de la présente invention, préférentiellement, le procédé est implémenté en tâche de fond pour ne pas perturber la communication normale entre le terminal et le site informatique, tant que la détection n'a pas eu lieu.

Pour chacun des aspects de la présente invention, un logiciel qui le met en oeuvre réside préférentiellement dans le terminal de l'utilisateur ou dans un serveur d'un fournisseur d'accès au réseau concerné.

En figure 1 sont représentés un terminal informatique 100, connecté, par l'intermédiaire d'un réseau 120, d'un serveur d'un fournisseur d'accès 130 et d'un réseau 140, à un site informatique distant 150, à un site tiers de protection 170 et à un site tiers de confiance 180. Dans le premier mode de réalisation illustré en figure 1, le terminal 100 comporte, reliés entre eux par un bus d'adresses et de données 109, une interface de communication sur un réseau 101, une unité de sauvegarde non volatile 102, un dispositif de pointage 103, un écran de visualisation 104, un clavier 105, une unité centrale 106, une mémoire centrale non volatile 107 et une mémoire vive 108.

Le réseau 120 est, par exemple, le réseau téléphonique commuté. Le serveur du fournisseur d'accès 130 est, par exemple, le serveur du fournisseur d'accès au réseau Internet connu sous le nom d'AOL (marque déposée) ou de WANADOO (marque déposée). Le réseau 140 est, par exemple, le réseau de communication informatique connu sous le nom d'Internet. Le site informatique distant 150 est mis en oeuvre par un serveur informatique ou un ordinateur programmé à cet effet selon des techniques connues.

Dans le premier mode de réalisation illustré en figure 1, le terminal 100 est un ordinateur personnel connu sous le nom de PC (acronyme de Personal Computer pour ordinateur personnel) ou un ordinateur de réseau, connu sous le nom de NC (acronyme de

Network Computer pour ordinateur de réseau). L'interface de communication sur un réseau 101 est, dans le premier mode de réalisation décrit et représenté, un modulateur-démodulateur ou MODEM. L'unité de sauvegarde non volatile 102, est, dans le premier mode de réalisation décrit et représenté, un disque dur ou un lecteur/enregistreur de disques compacts. Le dispositif de pointage 103, est, dans le premier mode de réalisation décrit et représenté, une souris informatique. L'écran de visualisation 104 est de type connu, par exemple à tube cathodique et compatible avec la norme connue de l'homme du métier sous le nom de SVGA.

Le clavier 105 comporte au moins des touches qui, seules ou en combinaison, permettent de sélectionner des caractères alphanumériques. L'unité centrale 106 est, dans le premier mode de réalisation décrit et représenté, un processeur, par exemple des marques déposées Intel Pentium. La mémoire centrale non volatile 107 conserve les instructions de programme du processeur 106 qui lui permettent de démarrer lorsqu'il commence à être alimenté en électricité. Le mémoire vive 108 est, dans le premier mode de réalisation décrit et représenté, une mémoire cache adaptée à conserver des informations représentatives d'au moins une page reçue de la part d'un site tel que le site informatique distant 150.

Le site tiers de protection 170 et le site tiers de confiance 180 possèdent, chacun un serveur qui conserve des pages Internet. En variante, au moins l'un de ces sites 170 et 180 est confondu avec celui du fournisseur d'accès 130.

La figure 2 représente ce qui est affiché par l'écran de visualisation 104 lorsque l'utilisateur du terminal 100 a sélectionné une offre commerciale de la part du site informatique distant 150 et que cet utilisateur s'apprête à effectuer un paiement en ligne, en fournissant des informations concernant une carte de paiement telles que le numéro et la date d'expiration de la carte de paiement.

De manière simplifiée, l'écran de visualisation 104 affiche alors :

- une portion principale 200 qui représente une portion d'une page reçue en provenance du site informatique distant 150 ;

- une bandeau supérieur 210 qui affiche, et permet de sélectionner, des fonctions ou des menus déroulants ;

- un bandeau inférieur 250 qui affiche des informations générales et des zones de sélection de fonction et

- un bandeau latéral 280 qui permet de faire défiler la page affichée dans la portion principale 200.

Dans l'exemple illustré en figure 2, la portion principale 200 comporte, au cours de la phase de la transaction qui correspond au début d'un paiement en ligne :

- une portion d'une page reçue en provenance du site informatique distant 150 comportant des informations textuelles d'une offre commerciale 220, éventuellement des informations graphique ou d'image (non représentées) et est associée à une séquence sonore (non représentée) ;

- des informations de sélection 230 d'au moins un autre page du site informatique distant 150 ;

- des conditions commerciales 235 ;

- un icône mobile 290 représentant la position sélectionnée par la souris 103 et

- une portion centrale de paiement en ligne 240.

La portion centrale 240 comporte, par exemple, des cases 241 de sélection d'un type de carte de paiement, une zone d'écriture 242 d'un numéro de carte de paiement, un zone d'écriture 243 d'un mois d'expiration de la durée de validité de carte de paiement et une zone de validation 244 de la saisie des informations relatives au paiement électronique en ligne et de la transaction.

Le bandeau supérieur 210 affiche deux flèches latérales 284 qui, lorsque l'une d'entre elles est sélectionnée par usage de la souris 103, permettent de retourner à la page précédemment affichée dans la portion centrale 200 (flèche orientée à gauche) ou d'avancer à la page affichée à la suite de la page en cours d'affichage dans la portion centrale 200 (flèche orientée vers la droite) selon des conventions connues dans les logiciels de navigation sur Internet. Le bandeau supérieur 210 affiche aussi des en-têtes de menus déroulant bien connus dans les logiciels de navigation, tels que :

- « fichier », pour créer, ouvrir, sauvegarder, imprimer ou fermer un fichier,

- « édition », pour sélectionner, couper, copier, coller, des informations,

- « accès Internet », pour rechercher un site Internet ou s'y connecter à partir de son adresse,

- « messagerie » pour accéder à sa messagerie personnelle, et

- « sites favoris », pour accéder directement à des sites Internet préalablement sélectionnés comme sites favoris.

L'utilisation de la souris 103 permet de sélectionner l'une des fonctions ou l'un des menus déroulants illustrés (parfois sous forme d'icônes) dans le bandeau supérieur 210.

Le bandeau latéral 280 comporte :

- une flèche supérieure 282 orientée vers le haut, dont la sélection provoque le défilement de la page illustrée dans la portion principale 200, vers le haut, pour en afficher sa partie supérieure,

- une flèche inférieure 283 orientée vers le bas, dont la sélection provoque le défilement de la page illustrée dans la portion principale 200, vers le bas, pour en afficher sa partie inférieure,

- une portion 281 qui, en combinaison avec une portion 284, représente la proportion de la page illustrée dans la portion principale 200 qui est affichée et

- une portion 284 qui représente, avec la même facteur de proportionnalité que la portion 281, la partie inférieure de la page illustrée dans la portion principale 200 qui n'est pas affichée.

Le bandeau inférieur 250 affiche des informations générales, telles que le nom du fournisseur d'accès, la durée de la connexion au fournisseur d'accès déjà écoulée, le logiciel de navigation utilisé (par exemple de l'une des marques déposées Netscape, Microsoft ou AOL) et des zones de sélection de fonction. Ici deux zones de sélection de fonctions 260 et 270 déclenchent une sauvegarde d'au moins une information de contenu d'au moins les portions des pages du site informatique distant 150 qui ont été reçues de la part du site informatique distant 150 et affichées sur l'écran de visualisation 104.

La zone 260 affiche, en clair, la fonction de sauvegarde sous la forme de deux mots « sauvegarde commerciale ». La zone 270 affiche, sous forme d'un icône représentant une balance, symbole de la justice, la fonction de sauvegarde. Selon différentes variantes de la présente invention :

- seules les portions qui ont été affichées,

- seules des informations de contenu ou de contexte, comme le nom du fournisseur et la date de la transaction,

- seuls certains mots présents dans ou représentant ces portions ou le fichier sonore reçu et diffusé,

- seuls les textes présents dans ces pages,

- les textes et les images,

- les pages entières,

- le fichier sonore,

- les informations de déplacement effectués dans les pages en cours d'affichage, et/ou

- la durée d'affichage de chaque portion de la page sur l'écran de visualisation 104

sont mis en mémoire non volatile, par exemple la mémoire 102 par déclenchement de la fonction de sauvegarde liée aux deux zones de sélection de fonctions 260 et 270.

Cette fonction et/ou d'autres fonctions de sécurisation sont aussi déclenchées de manière automatique par détection de préparation d'un paiement par transmission d'un identifiant de moyen de paiement au cours de la session de communication avec le site informatique distant 150, par l'intermédiaire du terminal 100, comme exposé en regard de l'opération 307, en regard des figures 3 et 4.

Selon un aspect de l'invention, et d'une manière générale, l'utilisateur met d'abord en fonctionnement un terminal informatique et accède, par l'intermédiaire d'un réseau de communication, à un site informatique distant.

Le terminal ouvre alors une session de communication avec le site informatique distant et reçoit, de la part du site informatique une offre de transaction. En tâche de fond, le terminal ou un système informatique par lequel transite des données échangées entre le terminal et le site informatique distant au cours de la session de communication, détermine si un paiement est préparé au cours de la session et par l'intermédiaire du terminal, par exemple en reconnaissant un identifiant d'une carte de paiement.

Si tel est le cas, le terminal ou le système informatique effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal. Cette opération de sécurisation comporte, au moins une opération de sauvegarde du montant du paiement, par exemple, en effectuant au moins l'une des opérations suivantes:

- création d'un fichier de sauvegarde et mise en mémoire d'au moins une parties des données au format « texte » échangées au cours de la session de communication entre le terminal et le site informatique ;

- constitution d'un message crypté représentatif d'au moins le montant de la transaction et, préférentiellement, d'un identifiant du fournisseur et transmission de ce message à un tiers de confiance comme, par exemple, un site informatique d'une banque auprès de laquelle le paiement doit être effectué ; et

- impression d'une trace de la transaction, comportant, au moins la date, le montant de la transaction, et, préférentiellement, le nom du fournisseur et un code d'intégrité (et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus) ; et

- constitution d'un message crypté représentatif d'au moins le montant de la transaction et, préférentiellement, d'un identifiant du fournisseur et transmission de ce message à un tiers de confiance comme, par exemple, un site informatique d'une banque auprès de laquelle le paiement doit être effectué ; et

- impression d'une trace de la transaction, comportant, au moins la date, le montant de la transaction, et, préférentiellement, le nom du fournisseur et un code d'intégrité (et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus) ; et

- affichage d'un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, et sauvegarde du contenu de ce questionnaire s'il a été au moins partiellement renseigné.

En outre, l'opération de sécurisation peut comporter l'une des opérations suivantes :

- authentification du payeur, par exemple par affichage d'une demande de code secret puis vérification du code secret ;

- affichage de données juridiques ;

- impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

- transmission au site informatique avec lequel la transaction est en cours, d'une information représentative de la sécurisation de la transaction, comme, par exemple, un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur.

Plus particulièrement, au cours d'un mode de fonctionnement du dispositif illustré en figure 1, l'utilisateur met en fonctionnement le terminal 100 et accède, par l'intermédiaire du modem 101 et du réseau 120, à un fournisseur d'accès à Internet 130.

Ensuite, l'utilisateur sélectionne, par l'intermédiaire du terminal 100, un site informatique distant 150, par exemple en pointant, avec la souris 103 :

- un identifiant d'un site dans le menu déroulant « sites favoris »,

- un lien avec un site sur le portail d'accès du fournisseur d'accès, ou

- le menu déroulant « accès Internet » et en saisissant une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Le terminal 100 entre alors en communication et ouvre une session de communication avec le site informatique distant 150 sélectionné, et lui envoie une information de sécurisation de transaction. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode de réalisation du procédé visé par la présente invention. Puis, le terminal 100 reçoit, de la part du site informatique

distant 150, une page Internet, par exemple une page d'accueil. Le terminal 100 provoque l'affichage, au moins partiel, de la page reçue. L'utilisateur peut alors déplacer cette page de manière à en prendre connaissance, plus ou moins complètement.

Ensuite, l'unité centrale 106 détermine si la page reçue est déjà conservée dans le disque dur 102, ou non. Si non, l'unité centrale 106 provoque la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, dans le disque dur 102. Ensuite ou si la page reçue est déjà conservée dans le disque dur 102, l'unité centrale 106 détermine si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page, tel que le lien 230.

Si l'utilisateur a sélectionné une autre page, et que la page sélectionnée n'a pas déjà été reçue au cours de la même session de communication entre le terminal 110 et le site informatique distant 150, le fonctionnement du terminal 100 déjà exposé ci-dessus est reproduit mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée en mémoire cache 108. Sinon, l'unité centrale 106 détermine si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement conservée en mémoire.

On observe ici que, par exemple lors de l'installation du logiciel qui permet l'application représentée ici, les quatre premiers chiffres des cartes de paiement de l'utilisateur lui sont demandées et sont mis en mémoire 102. Ensuite, en tâche de fond, chaque séquence de quatre chiffres saisis au clavier est comparée aux quatre premiers chiffres des cartes de paiement conservée en mémoire non volatile 102.

Si aucune séquence n'est reconnue, l'unité centrale 106 détermine si un autre site a été sélectionné par l'utilisateur, par exemple comme exposé ci-dessus ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la zone principale 200. Si tel est la cas, ce que le terminal 100 a effectué vis-à-vis du site en cours est reproduit vis-à-vis du nouveau site visité. Si aucun autre site n'a été sélectionné, l'affichage de la page est les opérations suivantes sont réitérées.

Lorsqu'une séquence correspondant, par exemple, aux quatre premiers chiffres d'un numéro de carte de paiement est reconnue, l'unité centrale 106 effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal. Cette opération de sécurisation comporte, au moins une sauvegarde locale ou à distance du

montant du paiement, par exemple, en effectuant au moins l'une des opérations exposées ci-dessous :

- l'unité centrale 106 provoque l'affichage d'une fenêtre sur l'écran 104, fenêtre comportant un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, le questionnaire portant, par exemple, sur le fournisseur, sur l'objet ou le service fournis, sur le montant de la transaction, sur le délai de fourniture, sur la garantie, sur le délai de réclamation, sur les conditions de remboursement en cas d'insatisfaction (pour remplir ce questionnaire, l'utilisateur peut minimiser la dimension de la fenêtre d'affichage du questionnaire et explorer les pages du site informatique distant 150) ;

- l'unité centrale 106 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les données au format « texte » des portions de pages du site informatique distant 150 qui ont été transmises au cours de la session de communication avec le site informatique distant 150. De manière préférentielle, cette mise en mémoire est associée à la mise en mémoire de la date. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit, au cours d'une lecture ultérieure, que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier. Le lecteur pourra, par exemple, s'inspirer des technique de marquage dites « watermarking » pour mettre en oeuvre cette fonction de code d'intégrité ;

- l'unité centrale 106 constitue un message crypté représentatif au moins du montant de la transaction et, préférentiellement d'un identifiant du fournisseur et ce message est transmis à un tiers de confiance 180, par exemple, le site informatique de la banque auprès de laquelle le paiement doit être effectué ; et/ou

- l'unité centrale 106 provoque l'impression de la date, du nom du fournisseur et du montant de la transaction, avec un code d'intégrité, et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus.

En outre, l'unité centrale 106 peut effectuer l'une des opérations suivante :

- l'unité centrale 106 affiche une demande de code secret (par exemple un nombre d'identification personnel connu sous le nom de PIN (pour Personal Identification Number) pour vérifier que l'utilisateur qui a saisi la séquence correspondant aux quatre premiers chiffres d'un numéro de carte de paiement est bien autorisé à utiliser cette carte, puis vérifie que ce code secret correspond à un code conservé en mémoire dans le disque dur 102 ;

- l'unité centrale 106 affiche une fenêtre comportant des données juridiques (voir figure 5) ; et

- l'unité centrale 106 effectue l'impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

L'unité centrale 106 envoie ensuite, au site informatique distant 150, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant 150. Cette information est, par exemple, identique à l'information déjà transmise au début de la session de communication. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. Ensuite l'unité centrale 106 détermine, comme ci-dessus, si un autre site a été sélectionné, ou non, et poursuit, comme ci-dessus, la séquence d'opération, en fonction du résultat de cette détermination. On observe que la fin de la session de communication, c'est à dire la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue, au cours de l'affichage de la dernière page reçue de la part du site informatique distant 150, et ne sont donc pas détaillées ici.

La figure 3 représente un organigramme mettant en oeuvre un mode de réalisation du procédé objet de la présente invention. Au cours d'une opération 300, il est accédé à un fournisseur d'accès à Internet.

Au cours de l'opération 301, un site informatique distant est sélectionné, par exemple par l'intermédiaire :

- d'un identifiant d'un site dans un menu déroulant,
- d'un lien avec un site sur le portail d'accès du fournisseur d'accès, ou
- d'une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Une session de communication est alors mise en place avec ce site informatique distant, au cours d'une opération 302, et une information de sécurisation de transaction est transmise au site informatique distant. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode de réalisation du procédé visé par la présente invention. Au cours de l'opération 303, il est reçu, de la part du site informatique distant 150, une page Internet qui, au cours de la première itération de la fonction 303, est une page d'accueil. Au cours de l'opération 304, un affichage, au moins partiel, de la page reçue au cours de l'opération 303 est effectué.

Au cours d'un test 305, il est déterminé si la page reçue est déjà mémorisée localement, ou non. Si le résultat du test 305 est négatif, au cours d'une opération 306, la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, d'une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, est effectuée. A la suite de l'opération 306 ou lorsque le résultat du test 305 est positif, au cours d'un test 307, il est déterminé si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page.

Lorsque le résultat du test 307 est positif et que la page sélectionnée n'a pas déjà été reçue au cours d'une opération 303, l'opération 303 est réitérée mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée localement. Lorsque le résultat du test 307 est négatif, au cours d'un test 308, il est déterminé si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement.

Par exemple, avant la mise en oeuvre du mode de réalisation du procédé exposé ici, les quatre premiers chiffres des cartes de paiement de l'utilisateur lui sont demandées et sont conservées localement. Dans cet exemple, au cours de l'opération 308, pour chaque saisie d'une séquence d'au moins quatre chiffres successifs, chaque séquence de quatre chiffres successifs de la séquence est comparé à la séquence de quatre chiffres conservée localement.

Lorsque le résultat du test 308 est négatif, au cours d'un test 309, il est déterminé si un autre site a été sélectionné, par exemple selon l'une des manières exposées en regard de l'opération 302 ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la page affichée, ou non. Lorsque le résultat du test 309 est positif, l'opération 302 est réitérée. Lorsque le résultat du test 309 est négatif, l'opération 304 est réitérée.

Lorsque le résultat du test 308 est positif, au cours d'une opération 310, une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur est effectuée en sauvegardant au moins le montant du paiement. Par exemple l'opération 310 comporte au moins l'une des opérations de sécurisation exposées ci-dessus.

A la suite de l'opération 310, au cours d'une opération 311, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant avec lequel la session a été ouverte au cours de l'opération 302. Cette information est, par exemple, identique à l'information transmise au cours de l'opération 301. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande

de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. A la suite de l'opération 311, le test 309 est effectué. On observe que la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue au cours de l'opération 304, et ne sont donc pas détaillées ici.

Lorsque le mode de réalisation du procédé illustré en figure 3 est mis en oeuvre par le mode de réalisation du dispositif illustré en figures 1 et 2, au cours d'une opération 300, l'utilisateur met en fonctionnement le terminal 100 et accède, par l'intermédiaire du modem 101 et du réseau 120, au fournisseur d'accès à Internet 130.

Au cours de l'opération 301, l'utilisateur sélectionne, par l'intermédiaire du terminal 100, un site informatique distant 150, par exemple en pointant, avec la souris 103 :

- un identifiant d'un site dans le menu déroulant « sites favoris »,
- un lien avec un site sur le portail d'accès du fournisseur d'accès, ou
- le menu déroulant « accès Internet » et en saisissant une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Le terminal 100 entre alors en communication avec le site informatique distant 150 sélectionné, au cours da l'opération 302, et lui envoie une information de sécurisation de transaction. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode de réalisation du procédé visé par la présente invention. Au cours de l'opération 303, le terminal 100 reçoit, de la part du site informatique distant 150, une page Internet qui, au cours de la première itération de la fonction 303, est une page d'accueil. Au cours de l'opération 304, le terminal 100 provoque l'affichage, au moins partiel, de la page reçue au cours de l'opération 303. Au cours de l'opération 304, l'utilisateur peut déplacer cette page de manière à en prendre connaissance, plus ou moins complètement, par l'intermédiaire de la souris 103 et de l'une des flèches 282 et 283.

Au cours du test 305, l'unité centrale 106 détermine si la page reçue est déjà conservée dans le disque dur 102, ou non. Si le résultat du test 305 est négatif, au cours d'une opération 306, l'unité centrale 106 provoque la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, dans le disque dur 102.

A la suite de l'opération 306 ou lorsque le résultat du test 305 est positif, au cours du test 307, l'unité centrale 106 détermine si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page, tel que le lien 230.

Lorsque le résultat du test 307 est positif et que la page sélectionnée n'a pas déjà été reçue au cours d'une opération 303, l'opération 303 est réitérée mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée en mémoire cache 108. Lorsque le résultat du test 307 est négatif, au cours du test 308, l'unité centrale 106 détermine si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement.

Lorsque le résultat du test 308 est négatif, au cours du test 309, l'unité centrale 106 détermine si un autre site a été sélectionné par l'utilisateur, par exemple selon l'une des manières exposées en regard de l'opération 302 ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la zone principale 200, ou non. Lorsque le résultat du test 309 est positif, l'opération 302 est réitérée. Lorsque le résultat du test 309 est négatif, l'opération 304 est réitérée.

Lorsque le résultat du test 308 est positif, au cours de l'opération 310, l'unité centrale 106 effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal 100 en sauvegardant au moins le montant du paiement. Cette opération de sécurisation comporte, par exemple, au moins l'une des opérations exposées ci-dessus. Par exemple, l'opération 310 comporte au moins l'une des opérations de protection suivantes:

- l'unité centrale 106 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les données au format « texte » des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 302 de connexion à ce site informatique distant 150. De manière préférentielle, cette mise en mémoire est associée à la mise en mémoire de la date. De manière préférentielle, au cours de l'opération 309, un code d'intégrité est inséré dans le fichier et garantit, au cours d'une lecture ultérieure, que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier. Le lecteur pourra, par exemple, s'inspirer des technique de marquage dites « watermarking » pour mettre en oeuvre cette fonction de code d'intégrité ;

- l'unité centrale 106 affiche une fenêtre comportant un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, le questionnaire portant, par

exemple, sur le fournisseur, sur l'objet ou le service fournis, sur le montant de la transaction, sur le délai de fourniture, sur la garantie, sur le délai de réclamation, sur les conditions de remboursement en cas d'insatisfaction (pour remplir ce questionnaire, l'utilisateur peut minimiser la dimension de la fenêtre d'affichage du questionnaire et explorer les pages du site informatique distant 150) ;

- l'unité centrale 106 constitue un message crypté représentatif au moins du montant de la transaction et, préférentiellement d'un identifiant du fournisseur et ce message est transmis à un tiers de confiance 180, par exemple, le site informatique de la banque auprès de laquelle le paiement doit être effectué ; et/ou

- l'unité centrale 106 provoque l'impression de la date, du nom du fournisseur et du montant de la transaction, avec un code d'intégrité, et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus.

En outre, cette opération de sécurisation comporte l'une des opérations ci-dessous :

- l'unité centrale 106 affiche une demande de code secret (par exemple un nombre d'identification personnel connu sous le nom de PIN (pour Personal Identification Number) pour vérifier que l'utilisateur qui a saisi la séquence reconnue au cours du test 308 est bien autorisée à le faire, puis vérifie que ce code secret correspond à un code conservé en mémoire dans le disque dur 102 ;

- l'unité centrale 106 affiche une fenêtre comportant des données juridiques (voir figure 5) ;

- l'unité centrale 106 effectue l'impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

A la suite de l'opération 310, au cours d'une opération 311, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant 150. Cette information est, par exemple, identique à l'information transmise au cours de l'opération 301. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. A la suite de l'opération 311, le test 309 est effectué. On observe que la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue au cours de l'opération 304, et ne sont donc pas détaillées ici.

Selon une variante non représentée, le test 308 et les opérations 309 et 310 sont effectuées par un système informatique par lequel transite les données échangées au cours de la session de communication ou les données envoyées par le terminal 100 au site informatique distant 150. Par exemple, le système informatique du fournisseur d'accès à Internet 130 peut effectuer ce test 308 et ces opérations 309 et 310 pour le compte de ses clients.

Selon un autre aspect du procédé visé par la présente invention, l'opération de sécurisation comporte :

- une connexion à un site tiers,

- une fourniture au site tiers d'un identifiant du site avec lequel la transaction est en cours (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), et un montant du paiement,

- une fourniture, par le site tiers, d'une information codée qui est représentative de la date et, préférentiellement, d'au moins un des identifiants indiqués ci-dessus selon une fonction de codage confidentielle,

- une création d'un fichier de sauvegarde conservant au moins les portions en mode « texte » des portions de pages transmises par le site informatique distant avec lequel la transaction est en cours, ainsi que l'information codée reçue de la part du site tiers. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier,

- une fourniture, par le site tiers, d'informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur, et

- un affichage d'informations légales.

Selon une variante, au moins une partie de l'identifiant d'un moyen de paiement, par exemple des chiffres de la carte de paiement ou une respectée par cette partie de l'identifiant, par exemple une somme des chiffres, sont transmis au site tiers et servent à calculer l'information codée.

Préférentiellement, la communication avec le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

Selon un autre aspect de la présente invention, le dispositif illustré en figure 1 et, plus particulièrement l'unité centrale 106 mettent en oeuvre les opérations exposées ci-dessus, si ce n'est que l'unité centrale 106 effectue une opération de sécurisation au cours de laquelle :

- le terminal 100 se connecte, par l'intermédiaire du réseau 140, au site tiers de protection 170,

- le terminal 100 fournit au site tiers de protection 170 un identifiant du site informatique distant 150 (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), un montant de transaction,

- le site tiers de protection 170 fournit une information codée qui est représentative de la date et, préférentiellement, d'au moins un des identifiants indiqués ci-dessus selon une fonction de codage confidentielle,

- le terminal 100 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les parties textuelles des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 302, ainsi que l'information codée reçue de la part du site tiers de protection 170. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier,

- le site tiers de protection 170 fournit au terminal 100 des informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur, et

- le terminal 100 provoque l'affichage d'informations légales (voir figure 5).

Selon une variante, au moins une partie d'un identifiant de moyen de paiement, ou une relation qu'elle respecte, par exemple le résultat de la somme de chiffres, est transmise au site tiers de protection 170 et sert à calculer l'information codée.

Préférentiellement, la communication entre le terminal 100 et le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

La figure 4 représente un organigramme d'opérations et tests d'un deuxième mode de réalisation du procédé objet de la présente invention. Cet organigramme comporte les même fonctions et tests que l'organigramme illustré en figure 3, à l'exception de l'opération 309 qui est remplacée par une opération 509, au cours de laquelle :

- le terminal 100 se connecte, par l'intermédiaire du réseau 140, au site tiers de protection 170 ;

- le terminal 100 fournit au site tiers de protection 170 un identifiant du site informatique distant 150 (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), et un montant du paiement ;

- le site tiers de protection 170 fournit une information codée qui est représentative de la date et, préférentiellement, des identifiants indiqués ci-dessus selon une fonction de codage confidentielle ;

- le terminal 100 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les parties textuelles des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 302, ainsi que l'information codée reçue de la part du site tiers de protection 170. De manière préférentielle, au cours de l'opération 309, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier ;

- le site tiers de protection 170 fournit au terminal 100 des informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur et

- le terminal 100 provoque l'affichage d'informations légales (voir figure 5).

Selon une variante, au moins une partie des chiffres de la carte de paiement qui sont conservés en mémoire 102 ou une relation entre eux, par exemple leur somme, sont transmis au site tiers de protection 170 et servent à calculer l'information codée.

Préférentiellement, la communication entre le terminal 100 et le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

Selon une variante non représentée, le site tiers de protection 170 crée un fichier de sauvegarde dans sa propre mémoire (non représentée) et y enregistre les informations reçues de la part du terminal 100. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier.

La figure 5 représente un écran de visualisation au cours de la mise en oeuvre du deuxième mode de réalisation du procédé objet de la présente invention, à la suite de l'opération 509.

L'écran de visualisation 104 présente les même éléments que ceux illustrés en figure 2, auxquels sont superposées, dans la portion principale 200, une fenêtre d'information complémentaire 750 et une fenêtre de questionnaire 760. La fenêtre d'information 750 comporte une indication 710 que des données liées à la transaction ont été enregistrées, une information sur la loi applicable à la transaction, 720, des informations légales minimales 730 et

740 comportant, en particulier, une information sur la durée de la garantie légale 730 et une information sur le délai légal maximal de réclamation concernant la transaction 740.

La fenêtre de questionnaire 760 comporte des textes indications permettant à l'utilisateur de renseigner des zones destinées à préciser des données liées à la transaction en cours. Dans l'exemple décrit et représenté, les renseignements suivants sont demandés à l'utilisateur :

- un code d'authentification, qui permet d'authentifier l'utilisateur de la carte de paiement ;
- un montant de paiement ;
- le nom du fournisseur ;
- l'objet ou le service obtenu en échange du paiement ;
- un délai d'alerte qui correspond à une date raisonnable ou l'utilisateur souhaite voir un message sur l'écran 104, par exemple à la mise en route de son terminal, message qui lui sert à vérifier si les obligations du fournisseur ont bien été honorées.

Les réponses à ce questionnaire sont mis en mémoire, localement et/ou par le biais d'un tiers de confiance, et, éventuellement, sont transmis (à l'exception du délai d'alerte) au site informatique distant 150.

Dans un autre mode de réalisation, tout ou partie de ces renseignements est automatiquement extrait des informations disponibles dans les pages reçues de la part du site informatique distant 150.

Selon une variante non représentée, la page fournie par le site informatique distant 150 comporte, de manière codée ou non, une information représentative de la date de la transaction ou un numéro de session et cette informations est mémorisée au cours de l'opération de sécurisation.

Selon d'autres variantes, les information mémorisées au cours de l'une des opérations 309 ou 509 sont représentatives des informations textuelles d'au moins une portion d'au moins une page fournie par le site informatique distant 150, portion qui a été affichée par l'écran 104, ou de l'une ou de plusieurs des informations suivantes :

- les informations textuelles des autres portions desdites pages,
- les informations textuelles des autres pages affichées par l'écran de visualisation 104 et fournies par le site informatique distant 150,
- des informations non textuelles (graphiques et images) desdites portions affichées,

- des informations non textuelles d'au moins deux pages fournies par le site informatique distant 150 et affichées par l'écran de visualisation 104,

- des informations non textuelles des autres pages fournies par le site informatique distant 150,

- des informations contextuelles, date, heure, autres sites visités précédemment, ...

L'opération de sécurisation peut aussi comporter un affichage d'informations concernant la propriété intellectuelle relative à la transaction en cours, un clôture de la session, une transmission d'un message court sur un réseau de télécommunication, tel qu'un réseau téléphonique, par exemple mobile, ou un réseau de pageur, à un terminal de communication de l'utilisateur, message récapitulant les informations principales de la transaction en cours, une opération de transfert de données (date, montant du paiement, fournisseur) à un logiciel de tenue de comptabilité, personnelle ou professionnelle.

Un mode de réalisation du logiciel qui implémente le procédé objet de la présente invention, peut comporter, dans son code informatique, une partie d'un identifiant de moyen de paiement afin que ce logiciel soit associé à la carte de paiement. Ainsi, le logiciel peut être fourni par l'organisme financier qui a fourni la carte de paiement à l'utilisateur ou le logiciel peut être vendu sur un réseau de communication, tout en empêchant une copie illégale de ce logiciel d'être utilisée avec une autre carte de paiement. Dans ce dernier cas, une détection d'un moyen de paiement autre que celui qui est associé au logiciel peut provoquer l'affichage d'un message invitant l'utilisateur à acquérir une version du logiciel associée au moyen de paiement qu'il tente d'utiliser. Lorsqu'une commission est prévue pour la sécurisation de données ou avec un tiers de confiance, le logiciel put aussi provoquer un paiement pour payer cette commission.

L'opération de sécurisation peut aussi comporter la génération d'un certificat de transaction, mettant en oeuvre un tiers de confiance selon des techniques connues. Par exemple, la détection du paiement peut provoquer l'émission par un tiers de confiance d'un identifiant de transaction qui est transmis à l'une ou l'autre des parties de la transaction en cours (par exemple le client), puis qui est retransmis entre les parties (par exemple au fournisseur) avant d'être utilisée pour obtenir le paiement.

Le procédé de l'invention peut être mis en oeuvre dans un logiciel comportant une fonction de fourniture d'une autorisation de paiement et, automatiquement, d'un identifiant d'un moyen de paiement. Ainsi, ce logiciel comporte une sécurisation conforme à ce qui est exposé ci-dessus. Dans ce cas, cependant, ce logiciel fonctionne, conformément à la présente

invention en tâche de fond par rapport à la session de communication entre le terminal et le site informatique distant.

On observe que l'information mémorisée au cours de l'opération de sécurisation peut être limitée au montant de la transaction et à une date, ou à ces éléments et un identifiant du fournisseur, ou à une seule page reçue de la part du site informatique distant 150 (par exemple la page de paiement, qui devrait légalement, à terme, récapituler les informations contractuelles).

La manière dont les informations enregistrées au cours de l'une des opérations de sécurisation exposées ci-dessus sont relues et mises à disposition de l'utilisateur, d'un avocat ou de la justice, sont bien connues de l'homme du métier et ne sont donc pas détaillées ici. D'une manière préférentielle, ces données ne peuvent pas être modifiées sans que cela ne soit perceptible.

En figure 6 sont représentées les opérations effectuées pour la mise en oeuvre du procédé visé par la présente invention tel qu'illustré en figures 1 à 5 et 7.

Au cours d'une opération 700, le logiciel mettant en oeuvre le procédé visé par la présente invention est installé.

Au cours de l'opération 710, l'utilisateur sélectionne un mode de détection de préparation de paiement. Par exemple l'utilisateur donne les quatre premiers numéros d'une carte de paiement ou sélectionne que tout quadruplet de séquences de quatre chiffres ou une fonction d'un logiciel de paiement ou la sélection d'un icône dédié au paiement (non représenté) seront à détecter comme préparation d'un paiement en ligne.

Au cours de l'opération 710, l'utilisateur sélectionne aussi les fonctions d'une opération de sécurisation, parmi celles qui sont exposées ci-dessus. L'opération de sécurisation comporte, au moins une opération de sauvegarde du montant du paiement. L'utilisateur peut aussi choisir un code secret, s'il souhaite être authentifié à chaque paiement en ligne. L'utilisateur peut aussi choisir un tiers de confiance et un organisme financier. L'utilisateur désigne aussi un ou plusieurs logiciels de navigation sur un réseau de communication informatique tel qu'Internet. Le mode de fonctionnement sélectionné par l'utilisateur est mis en mémoire.

Au cours d'une opération 720, à chaque mise en fonctionnement du terminal 100 ou à chaque lancement de l'un des logiciels de navigation désignés au cours de l'opération 710, la fonction de détection de paiement et, en cas de détection, la fonction de sécurisation, sont

mises en fonctionnement en tâche de fond. Des modes d'implémentation de l'opération 720 sont décrits en regard des figures 3 et 4.

Au cours d'un test 730, il est détecté si une période bancaire, par exemple la période facturation de l'utilisation d'une carte de paiement, a expiré, ou non. Si le résultat du test 730 est négatif, l'opération 720 est réitérée. Si le résultat du test 730 est positif, un affichage et/ou une impression de tous les achats effectués au cours de la période bancaire considérée est effectuée au cours d'une opération 740, puis l'opération 720 est réitérée.

On observe que la détection de la préparation de paiement peut consister en une détection d'un paiement, par exemple, par détection de transmission, sur le bus 109, d'informations relative à un moyen de paiement ou par détection de mise en fonctionnement d'un logiciel ou d'une routine de paiement ou de comptabilisation.

Revendications

1. Procédé de sécurisation, caractérisé en ce qu'il comporte :

- une opération (800) d'ouverture d'une session de communication entre un terminal (100) informatique et un site informatique (150), par l'intermédiaire d'un réseau de communication (140),

- une opération (820) de détection automatique d'une préparation de paiement (810) par transmission, au cours de ladite session, par l'intermédiaire dudit terminal, d'un identifiant d'un moyen de paiement, et

- lorsqu'une préparation de paiement est détectée, une opération (830) automatique de sécurisation dudit paiement en dehors dudit site informatique, ladite opération de sécurisation comportant au moins une opération de sauvegarde du montant du paiement en dehors dudit site informatique.

2. Procédé selon la revendication 1, caractérisé en ce que l'opération de détection de préparation d'un paiement comporte une opération de détection d'un identifiant d'un moyen de paiement.

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte une opération de saisie de symboles par l'intermédiaire d'un clavier dudit terminal, et l'opération de détection comporte une opération de reconnaissance, parmi les symboles saisis au cours de l'opération de saisie, de tout ou partie :

- d'un numéro de carte de paiement ou de crédit,

- d'une date de péremption d'une telle carte, et/ou

- d'un numéro de compte bancaire.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que l'opération de reconnaissance comporte une opération de comparaison d'une succession de symboles saisis et d'au moins une séquence de symboles conservée en mémoire.

5. Procédé selon la revendication 4, caractérisé en ce que l'opération de reconnaissance comporte une opération de détection d'une succession de symboles saisis présentant une caractéristique prédéterminée.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que l'opération de sécurisation comporte :

- une opération de mise en mémoire de données échangées avec un format « texte » au cours de la session de communication, et/ou

- une opération de communication à un tiers de confiance, de données relatives au paiement.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que l'opération de détection est effectuée en tâche de fond par rapport à la session de communication et l'opération de préparation de paiement.

8. Dispositif de sécurisation, caractérisé en ce qu'il comporte :

- un terminal informatique qui ouvre une session de communication avec un site informatique, par l'intermédiaire d'un réseau de communication,

- un moyen de détection automatique de préparation d'un paiement par l'intermédiaire du terminal, et

- un moyen de sécurisation dudit paiement, lorsqu'une préparation de paiement est détectée comportant un moyen de sauvegarde d'au moins un montant de paiement en dehors du site informatique distant.

9. Dispositif de sécurisation selon la revendication 8, caractérisé en ce que le moyen de détection et le moyen de sécurisation sont dans le terminal informatique.

10. Dispositif de sécurisation selon la revendication 8, caractérisé en ce que le moyen de détection et le moyen de sécurisation sont dans un système informatique d'un fournisseur d'accès du terminal audit réseau.

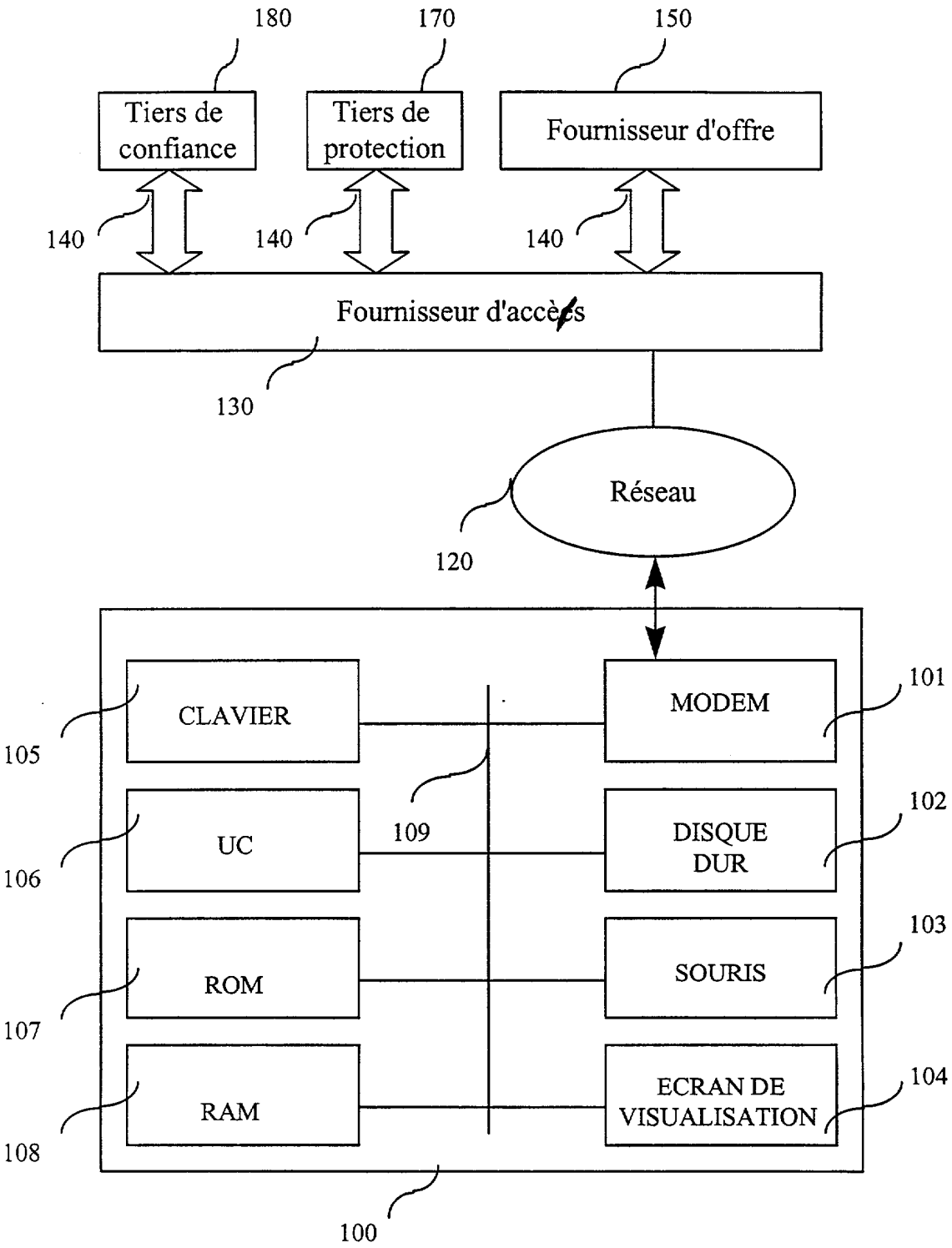

180
170
150
Tiers de confiance
Tiers de protection
Fournisseur d'offre
140
140
140
Fournisseur d'accès
130
Réseau
120
CLAVIER
MODEM
101
105
109
UC
DISQUE DUR
102
106
ROM
SOURIS
103
107
RAM
ECRAN DE VISUALISATION
104
108
100

Fig. 1

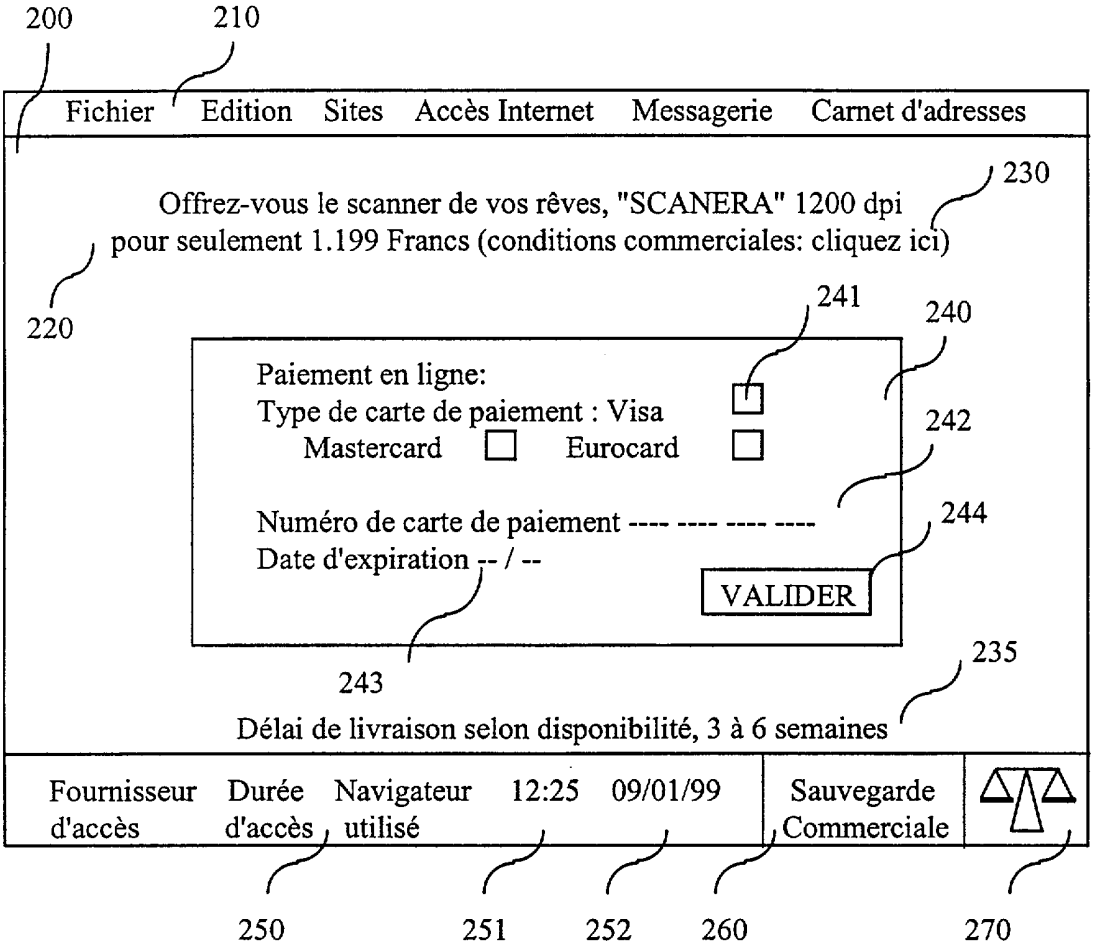

200
210
Fichier
Edition
Sites
Accès Internet
Messagerie
Carnet d'adresses
230
Offrez-vous le scanner de vos rêves, "SCANERA" 1200 dpi
pour seulement 1.199 Francs (conditions commerciales: cliquez ici)
220
241
240
Paiement en ligne:
Type de carte de paiement : Visa
Mastercard
Eurocard
242
Numéro de carte de paiement ---- ---- ---- ----
244
Date d'expiration -- / --
VALIDER
243
235
Délai de livraison selon disponibilité, 3 à 6 semaines
Fournisseur d'accès
Durée d'accès
Navigateur utilisé
12:25
09/01/99
Sauvegarde Commerciale
250
251
252
260
270

Fig. 2

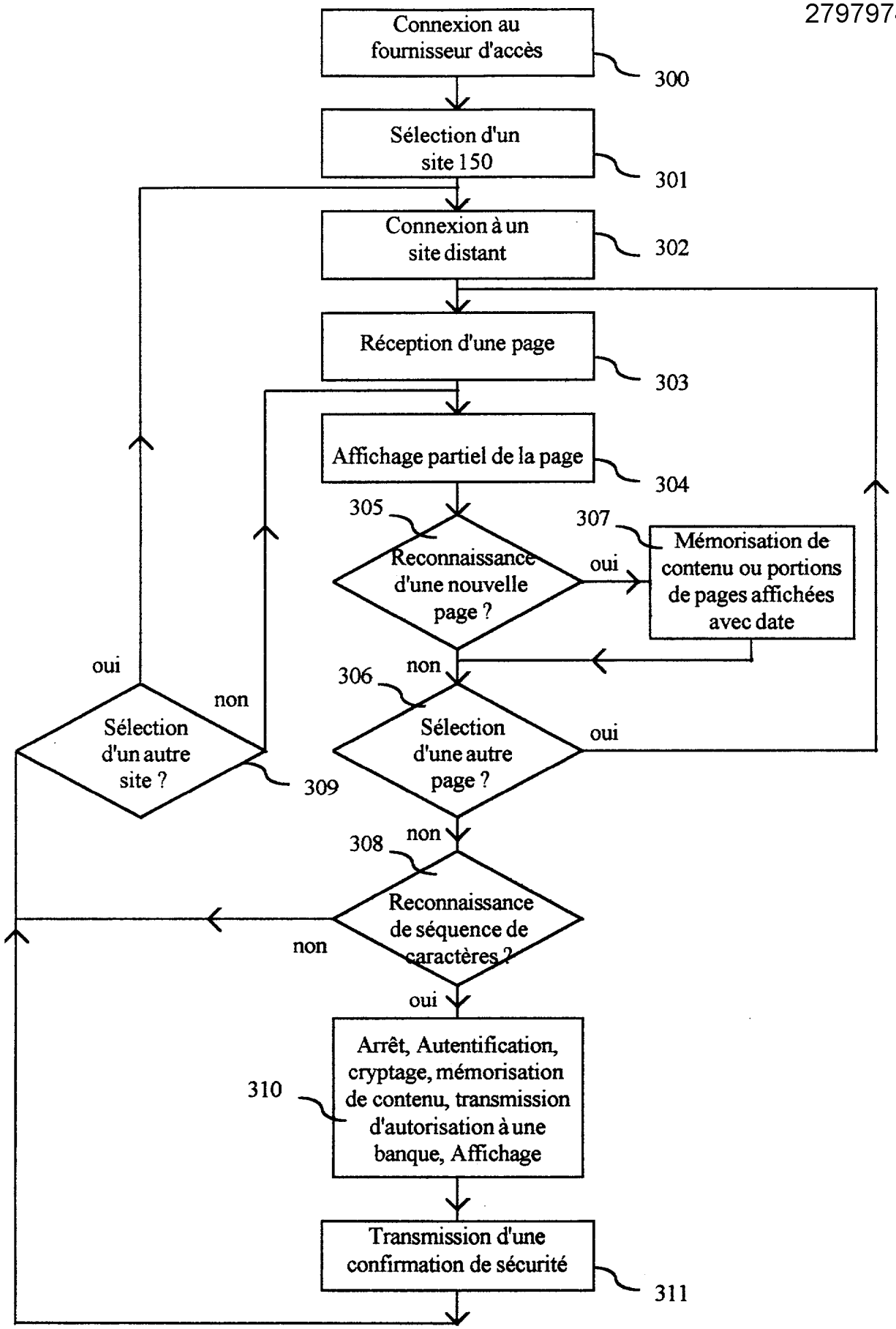

Connexion au fournisseur d'accès
300
Sélection d'un site 150
301
Connexion à un site distant
302
Réception d'une page
303
Affichage partiel de la page
304
305
Reconnaissance d'une nouvelle page ?
oui
307
Mémorisation de contenu ou portions de pages affichées avec date
non
306
Sélection d'une autre page ?
oui
non
308
Reconnaissance de séquence de caractères ?
non
oui
Arrêt, Autentification, cryptage, mémorisation de contenu, transmission d'autorisation à une banque, Affichage
310
Transmission d'une confirmation de sécurité
311
oui
non
Sélection d'un autre site ?
309

Fig. 3

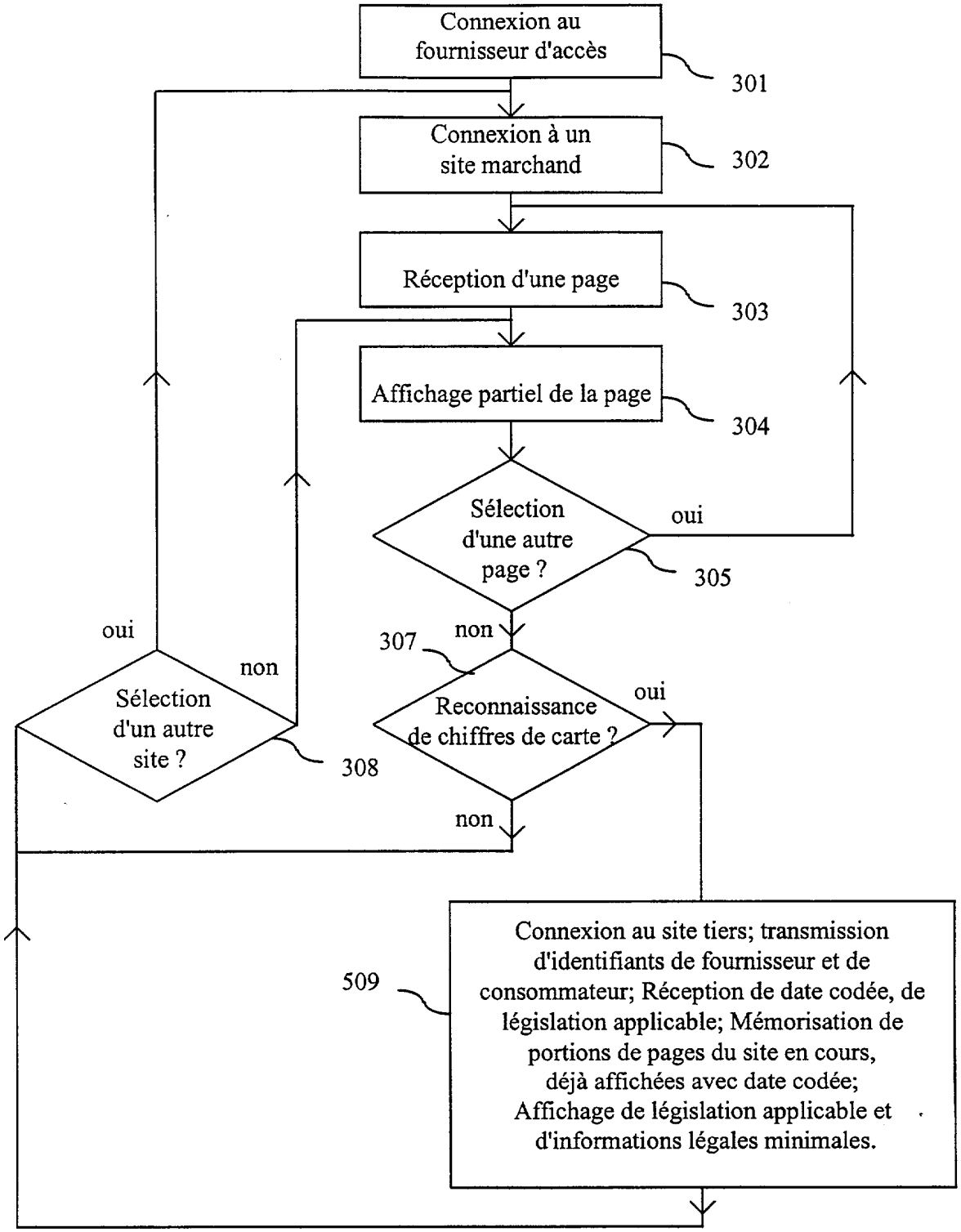

Connexion au fournisseur d'accès
301
Connexion à un site marchand
302
Réception d'une page
303
Affichage partiel de la page
304
Sélection d'une autre page ?
oui
305
non
307
Reconnaissance de chiffres de carte ?
oui
non
Sélection d'un autre site ?
oui
non
308
509
Connexion au site tiers; transmission d'identifiants de fournisseur et de consommateur; Réception de date codée, de législation applicable; Mémorisation de portions de pages du site en cours, déjà affichées avec date codée; Affichage de législation applicable et d'informations légales minimales.

Fig. 4

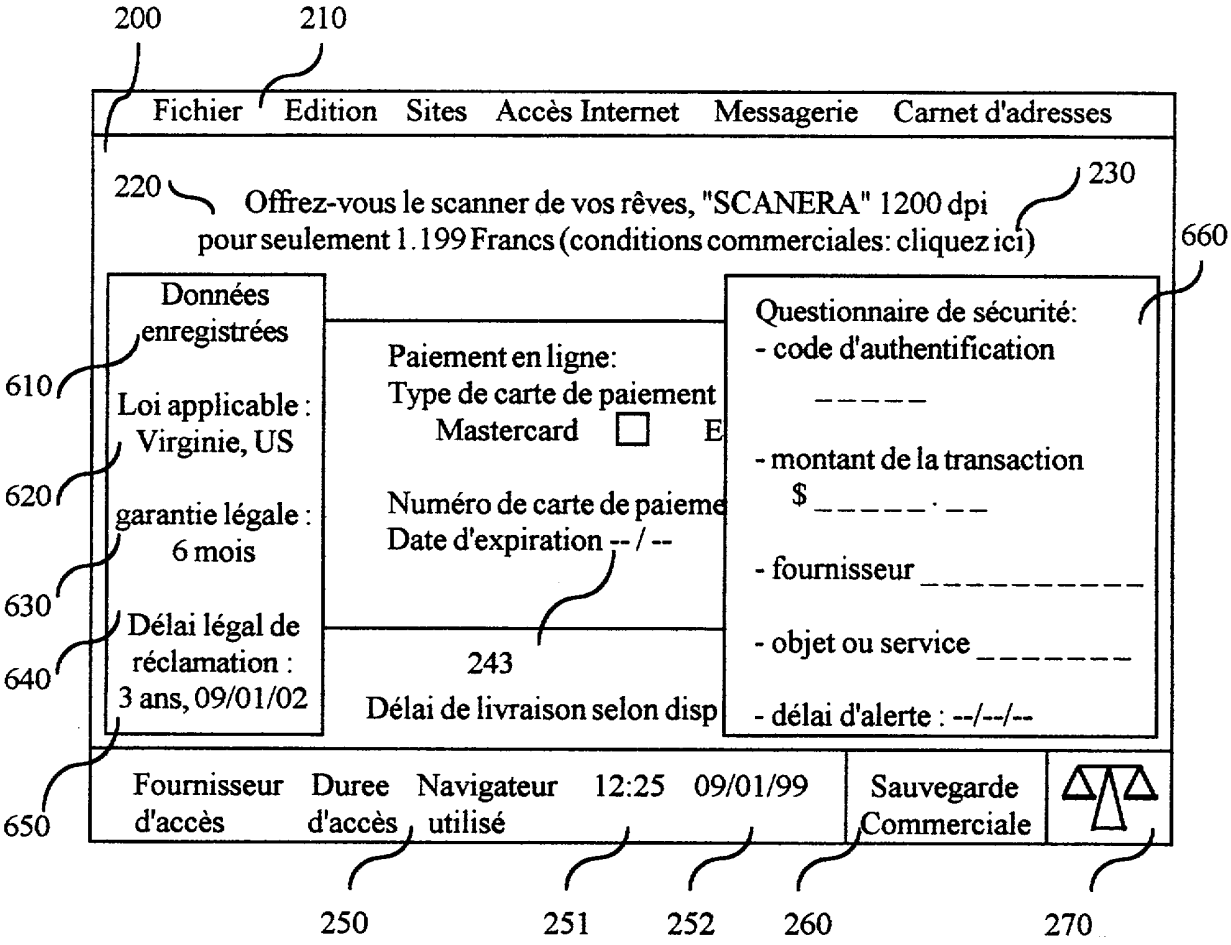

200
210
Fichier
Edition
Sites
Accès Internet
Messagerie
Carnet d'adresses
220
Offrez-vous le scanner de vos rêves, "SCANERA" 1200 dpi
pour seulement 1.199 Francs (conditions commerciales: cliquez ici)
230
660
Données enregistrées
610
Loi applicable : Virginie, US
620
garantie légale : 6 mois
630
Délai légal de réclamation : 3 ans, 09/01/02
640
650
Paiement en ligne:
Type de carte de paiement
Mastercard
E
Numéro de carte de paieme
Date d'expiration -- / --
243
Délai de livraison selon disp
Questionnaire de sécurité:
- code d'authentification
_ _ _ _ _
- montant de la transaction
$ _ _ _ _ _ . _ _
- fournisseur _ _ _ _ _ _ _ _ _
- objet ou service _ _ _ _ _ _ _
- délai d'alerte : --/--/--
Fournisseur d'accès
Duree d'accès
Navigateur utilisé
12:25
09/01/99
Sauvegarde Commerciale
250
251
252
260
270

Fig. 5

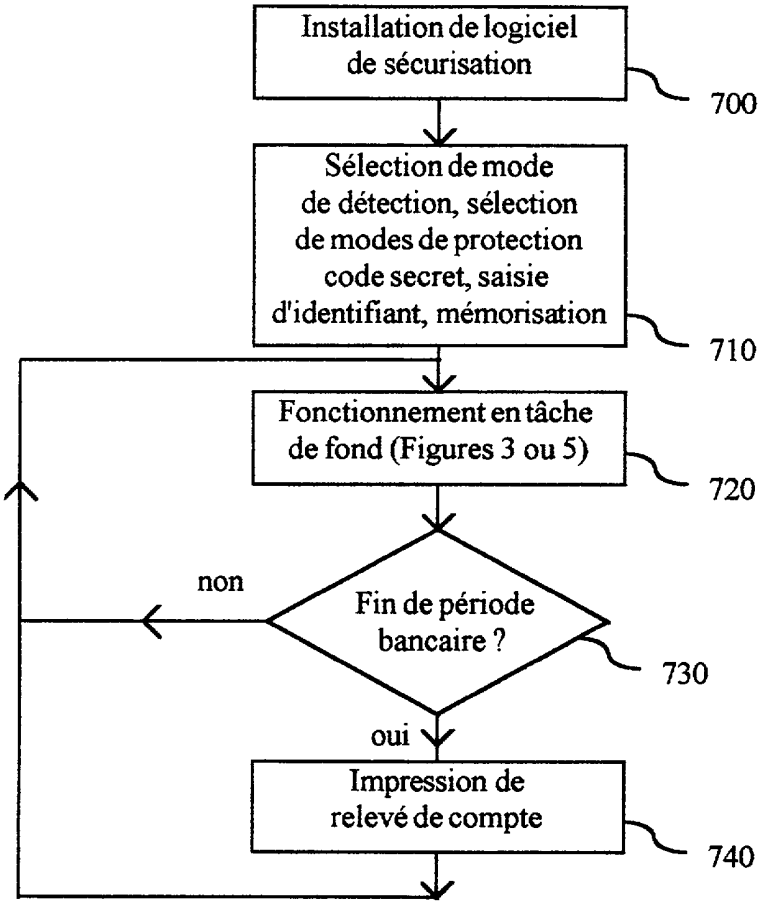

Installation de logiciel de sécurisation
700
Sélection de mode de détection, sélection de modes de protection code secret, saisie d'identifiant, mémorisation
710
Fonctionnement en tâche de fond (Figures 3 ou 5)
720
non
Fin de période bancaire ?
730
oui
Impression de relevé de compte
740

Fig. 6

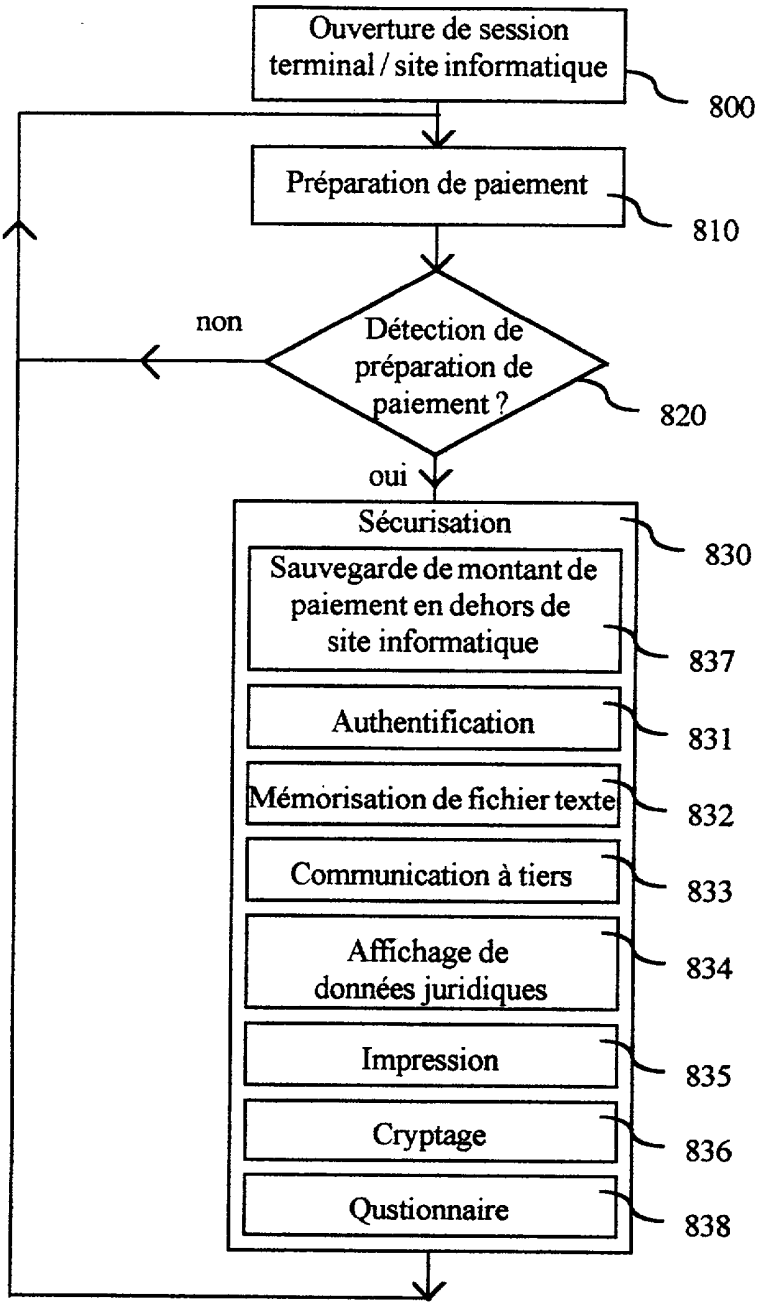

Ouverture de session terminal / site informatique
800
Préparation de paiement
810
non
Détection de préparation de paiement ?
820
oui
Sécurisation
830
Sauvegarde de montant de paiement en dehors de site informatique
837
Authentification
831
Mémorisation de fichier texte
832
Communication à tiers
833
Affichage de données juridiques
834
Impression
835
Cryptage
836
Qustionnaire
838

Fig. 7

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2797974

N° d'enregistrement national

FA 578011
FR 9912108

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 95 16971 A (OPEN MARKET INC) 22 juin 1995 (1995-06-22) * page 5, ligne 8 - page 6, ligne 39 * * page 9, ligne 31 - page 10, ligne 11 * * page 11, ligne 9 - ligne 13 * * page 14, ligne 24 - ligne 29 * * page 15, ligne 29 - page 16, ligne 23 * * page 18, ligne 10 - ligne 18 * ---	1-10
X	US 5 715 314 A (MACKIE DAVID J ET AL) 3 février 1998 (1998-02-03) * colonne 6, ligne 9 - ligne 30 * ---	1,3,8-10
X	US 5 826 241 A (STEFFERUD EINAR A ET AL) 20 octobre 1998 (1998-10-20)	1,7-10
A	* colonne 3, ligne 38 - ligne 46 * * colonne 5, ligne 27 - ligne 37 * * colonne 6, ligne 47 - colonne 7, ligne 25 * * colonne 8, ligne 51 - ligne 54 * * colonne 9, ligne 55 - colonne 10, ligne 8 * * revendications 1-3 * ---	2-6
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 mars 1999 (1999-03-16) * colonne 1, ligne 65 - colonne 2, ligne 67 * * revendication 36 * ---	
A	EP 0 927 945 A (AMAZON COM INC) 7 juillet 1999 (1999-07-07) -----	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)
G07F G06F

Date d'achèvement de la recherche	Examinateur
30 mai 2000	Wolles, B

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)