

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 02.08.01.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 07.02.03 Bulletin 03/06.

(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) : GROSS GABRIEL — FR.

(72) Inventeur(s) : GROSS GABRIEL.

(73) Titulaire(s) :

(74) Mandataire(s) : CABINET PLASSERAUD.

(54) PROCÉDÉ DE COMMUNICATION POUR ÉCHANGER DE MANIÈRE CONTRÔLÉE DES DONNÉES ENTRE UN TERMINAL CLIENT ET UN RÉSEAU DE SITES HÔTES ET ENSEMBLE SERVEUR DE PROTECTION POUR LA MISE EN OEUVRE DE CE PROCÉDÉ.

(57) Procédé de communication pour échanger de manière contrôlée des données entre un terminal client (1) et un réseau de sites (2) hôtes dans lequel :

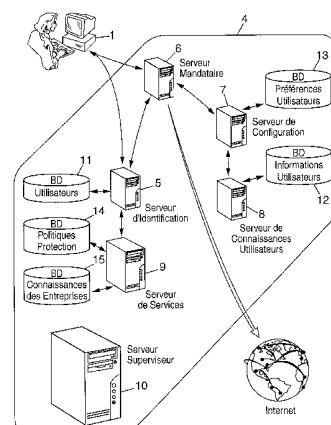
- les données sont échangées, entre le terminal client (1) et le réseau, par l'intermédiaire d'un serveur de protection (6),

- l'identifiant du terminal client est masqué, vis-à-vis du réseau, au niveau du serveur de protection (6), et

- au moins une partie des données sont protégées de la lecture par une personne non autorisée à la lire, lorsque ces données sont communiquées entre le serveur de protection (6) et le terminal client (1).

Le contrôle des échanges de données est en particulier réalisé grâce à un moteur d'inférence d'un statut de confiance établi pour les sites hôtes (2).

Dispositif pour la mise en oeuvre de ce procédé.



Procédé de communication pour échanger de manière contrôlée des données entre un terminal client et un réseau de sites hôtes et ensemble serveur de protection pour la mise en œuvre de ce procédé

5

L'invention est relative à un procédé de communication pour échanger, de manière contrôlée, des données entre un terminal client et un réseau de sites hôtes, ainsi qu'à un ensemble serveur de protection pour la mise en œuvre de ce procédé.

Dans ce document, le terme « terminal » désigne un micro-ordinateur, un téléphone mobile, ou tout autre dispositif apte à communiquer avec un réseau de serveurs de données.

Dans une application particulière, le procédé selon l'invention est destiné à permettre à un internaute de contrôler la diffusion sur Internet, des informations qui le concernent.

D'une part, un internaute peut, par exemple afin de bénéficier de services personnalisés, être amené à transmettre à un site hôte certaines données sur son identité, ses revenus, ses préférences en terme de loisirs, de shopping, etc., mais néanmoins souhaiter que ces informations ne soient pas utilisées pour d'autres fins que celles pour lesquelles il les a révélées.

D'autre part, certains sites envoient, à destination des terminaux des internautes qui se connectent à eux, des témoins, aussi appelés « cookies », pour les installer automatiquement sur ces terminaux. Ces cookies sont des fichiers, qui une fois enregistrés dans la mémoire de ces terminaux, permettent au serveur du site qui les a émis de recevoir des informations sur l'internaute et son comportement. Les internautes souhaitent parfois éviter

l'installation de cookies sur leur terminal et éviter, sans perdre nécessairement pour autant toute possibilité de bénéficier de services personnalisés, que des informations qui les concernent soient recueillies et utilisées à leur 5 insu.

On connaît déjà, par le document EP-A-1 017 205, un procédé pour fournir anonymement des informations sur l'internaute, lorsqu'il navigue sur Internet. Dans ce procédé de l'art antérieur, on enregistre les informations 10 dans une mémoire, on génère un pseudonyme pour l'internaute, on lie ce pseudonyme aux informations contenues dans la mémoire, dans un registre et on transmet le registre, automatiquement ou en réponse aux commandes de l'internaute, aux sites consultés par celui-ci. Ces sites n'ont donc accès 15 aux informations en question qu'en liaison avec le pseudonyme. Un tel pseudonyme est généralement lié à un avatar, c'est à dire une représentation virtuelle créée par l'internaute pour évoluer dans le cyberspace.

Cependant un tel procédé ne permet notamment pas 20 d'éviter que le fournisseur d'accès à Internet (aussi appelé par l'homme du métier « ISP », pour Internet Service Provider), auquel est abonné l'internaute, n'ait connaissance de l'identité des sites consultés par ce dernier.

25 On connaît également des logiciels qui, une fois installés sur le terminal de l'internaute, permettent à ce dernier de sélectionner les cookies qu'il veut bien voir enregistrés sur son terminal.

Cependant, de tels logiciels n'offrent aucune 30 protection des données transmises sur le réseau, à partir du terminal de l'internaute, que ce soit à partir de celles recueillies grâce aux cookies ou les autres.

Il y a aussi un besoin en procédés et dispositifs de protection de la vie privée des internautes qui permettent éventuellement une offre de services personnalisés.

5 Un but de l'invention est notamment de fournir un procédé de communication de données entre un terminal client et un réseau de sites hôtes, permettant une meilleure protection de ces données, vis-à-vis de leur utilisation par des tiers non autorisés et qui, préférentiellement, autorise l'offre de services personnalisés.

10 Ce but est atteint, selon l'invention, grâce à un procédé de communication pour échanger de manière contrôlée des données entre un terminal client et un réseau de sites hôtes, ce procédé étant caractérisé par le fait que :

15 - les données sont échangées, entre le terminal client et le réseau, par l'intermédiaire d'un serveur de protection,

- l'identifiant du terminal client est masqué, vis à vis du réseau, au niveau du serveur de protection,

20 - au moins une partie des données est protégée de la lecture par toute personne non autorisée à lire cette partie des données, lorsque ces données sont communiquées entre le serveur de protection et le terminal client ;

25 - un profil de préférences qualifiant un utilisateur du terminal client et agréé par cet utilisateur est comparé à des connaissances sur au moins un site hôte, et

- l'échange des données entre le terminal client et ce site hôte est contrôlé en fonction d'informations issues de cette comparaison.

En effet, selon ce procédé :

30 - d'une part, entre le terminal client (un terminal d'internaute par exemple), et le serveur de protection, les données échangées sont rendues, au moins en partie, voire

5 totalement, confidentielles par la protection d'au moins une partie de celles-ci ; ainsi lorsque l'utilisateur accède au serveur de protection grâce à un fournisseur d'accès au réseau, les données échangées entre le serveur de protection et le terminal client sont au moins en partie protégées de la lecture par le fournisseur d'accès ; et

10 - d'autre part, l'identifiant du terminal client (adresse IP pour un terminal connecté à Internet ; IP étant l'acronyme de « Internet Protocol ») est masqué et les données transmises entre le terminal client et le reste du réseau sont soumises à un contrôle, en fonction de ce que l'utilisateur souhaite, parmi les informations qui le concernent, diffuser ou non sur le réseau.

15 Ainsi, certaines des données qui concernent l'utilisateur peuvent, si ce dernier le souhaite, n'être connues, ni des tiers exploitant les sites visités par celui-ci, ni des tiers qui envoient des cookies à destination du terminal de l'internaute sans que ce dernier ait choisi de se connecter à un site de ces tiers (par exemple les régies publicitaires), ni même de son fournisseur d'accès.

20 Dans des modes de réalisation préférés, le procédé selon l'invention comporte l'une et/ou l'autre des caractéristiques suivantes :

25 - des adresses de sites hôtes à destination desquels sont envoyées des données, à partir du terminal client, sont dissimulées au fournisseur d'accès ; dans le cadre d'une connexion à Internet ces adresses sont des adresses URL (Acronyme de l'expression anglo-saxonne « Uniform Ressource Locator ») ;

30 - le serveur de protection fournit sur requête, à la place du fournisseur d'accès, une adresse de site hôte

identifié par un nom, en correspondance de ce nom, à l'aide d'un système de noms de domaine ; ainsi dans le cadre d'une connexion à Internet, ce système de noms de domaine est appelé DNS (Acronyme de l'expression anglo-saxonne « Domain Naming System ») ;

5 - une partie, comportant des informations sur l'identité du terminal client, d'une requête formulée à partir du terminal client à destination d'un site hôte, est modifiée, voire éliminée, avant de transiter vers le site 10 hôte auquel est destinée la requête ; ainsi dans le cadre d'une connexion à Internet, c'est une partie de l'en-tête (aussi appelé « header » par l'homme du métier) de la requête qui fait l'objet de cette modification ;

15 - il comporte un filtrage de témoins (cookies) en provenance du réseau par le serveur de protection, et un stockage, au niveau du serveur de protection, d'au moins une partie de ces témoins ; certains témoins sont éliminés tandis que d'autres sont enregistrés au niveau du serveur de protection ; aucun témoin n'est stocké sur le terminal 20 client, mais l'utilisateur peut néanmoins profiter des avantages que procurent certains de ces témoins, comme l'offre de services personnalisés en fonction du profil d'informations attaché directement à son identité ou à l'(aux) avatar(s) qui le représente(nt) ;

25 - un serveur de courrier électronique fournit au moins une adresse de courrier électronique à usage unique ;

- il comprend un suivi de l'utilisation de l'adresse à usage unique, faite par un tiers à qui cette adresse de courrier électronique a été transmise ;

30 - une pluralité de comptes de messagerie électronique est attribuée à un utilisateur, avec un portail

unique, indépendant du terminal client et personnel pour gérer ces comptes ;

5 - un statut de confiance est associé à un site hôte, en fonction de connaissances, stockées dans une base de connaissances, sur au moins la politique de protection des données personnelles par un tiers exploitant ce site hôte ; cette politique est par exemple définie d'une part, par un formulaire P3P (De « Platform for Privacy Preference Project ») qualifiant un site, et d'autre part, par des tests sur l'utilisation des informations par ce site et/ou 10 par des connaissances générales (réputation par exemple) de l'entreprise qui exploite ce site ;

15 - un formulaire de saisie d'informations sur l'utilisateur, fourni par un site hôte et destiné à l'enregistrement des informations saisies, par ce site hôte, est rempli automatiquement par le serveur de protection en fonction du statut de confiance, avant d'être soumis à 20 l'approbation de l'utilisateur ;

- l'approbation par l'utilisateur est réalisée automatiquement en fonction d'un profil de protection qu'il 25 a prédefini ;

- l'utilisateur du terminal client est représenté, vis-à-vis du réseau, par au moins un avatar ; ainsi l'utilisateur peut diffuser des données qualifiantes, par exemple sur ses préférences, sans que celles-ci soient nécessairement attachées à son identité réelle ;

30 - un profil d'informations comprenant le profil de préférences et associé à l'identité réelle de l'utilisateur ou à chaque avatar est stocké au niveau d'une base de connaissances, ce profil étant déterminé, au moins en partie, par le comportement de l'utilisateur lorsqu'il communique avec le réseau en utilisant cet avatar ; ainsi,

les préférences associées à l'avatar de l'utilisateur peuvent être prises en compte dans ce profil ; le profil d'informations comporte les données qualifiantes sur l'utilisateur, associées à cet avatar ;

5 - le profil d'informations est modifié par l'utilisateur par l'intermédiaire d'un serveur de configuration ; ceci permet à l'utilisateur de modifier les données qui le concernent enregistrées dans ce profil d'informations, par exemple, pour affiner ce profil en vue 10 d'une amélioration de la personnalisation des services qui peuvent lui être offerts ou pour supprimer de ce profil des informations qu'il ne souhaite pas voir diffusées ;

15 - une autorisation d'utilisation, par un tiers exploitant un site hôte, des informations attachées à l'identité réelle de l'utilisateur ou à l'avatar sous lequel l'utilisateur accède à ce site hôte est régie par l'utilisateur, au moyen de la sélection et de l'activation d'un profil de protection prédefini ; par exemple, l'utilisateur peut ainsi choisir un profil « paranoïaque » 20 qui lui permet par exemple de refuser automatiquement et systématiquement la transmission d'une quelconque information qui le concerne, un profil « normal » qui lui permet d'accepter que certaines informations soient communiquées seulement si le site auquel elles sont 25 destinées bénéficie d'une certaine confiance, ou un profil « souple » qui lui permet d'accepter que n'importe quelle information attachée à l'avatar qu'il utilise soit transmise au(x) sites(s) au(x)quel(s) il se connecte ;

30 - le profil de protection est confronté au statut de confiance pour définir un traitement automatique des données échangées entre ce site hôte et le terminal client, lorsque l'utilisateur souhaite établir une communication avec un

site hôte et préalablement à cette communication, et/ou lorsqu'un site hôte souhaite entrer en communication avec le terminal client (par exemple, une régie publicitaire) ; et

5 - le traitement automatique des données échangées entre le site hôte et le terminal client comporte le filtrage de témoins en provenance du réseau et le stockage, au niveau du serveur de protection, d'au moins une partie des témoins filtrés ; ainsi par exemple, si l'utilisateur choisit un profil « paranoïaque », tout témoin en provenance d'un site ayant un faible statut de confiance est refusé, alors qu'avec un profil « normal », il peut accepter automatiquement les témoins provenant de ce site hôte qui sont détruits en fin de session de connexion avec ce dernier, ou un profil « souple » qui lui permet d'accepter 10 le stockage de n'importe quel témoin provenant de ce site.

15

Selon un autre aspect, l'invention propose un ensemble serveur de protection pour faire l'interface entre un terminal client et un réseau de sites hôtes et permettre à un utilisateur du terminal client de contrôler la diffusion d'informations qui le concernent, sur le réseau, cet ensemble serveur de protection comportant :

20 - des moyens, au niveau d'un serveur de protection, pour masquer l'identifiant du terminal client, vis-à-vis du réseau,

25 - des moyens pour protéger, au moins une partie des données, de la lecture par toute personne non autorisée à lire cette partie des données, lorsque ces données sont communiquées entre le serveur de protection et le terminal client,

30 - des moyens de comparaison pour comparer, à des connaissances sur au moins un site hôte, un profil de

préférences qualifiant l'utilisateur et agréé par ce dernier, et

5 - des moyens pour contrôler, en fonction d'informations générées par les moyens de comparaison, l'échange des données entre le terminal client et ce site hôte.

Dans des modes de réalisation préférés, le procédé selon l'invention comporte l'une et/ou l'autre des caractéristiques suivantes :

10 - il comporte des moyens pour créer au moins un avatar permettant de représenter l'utilisateur vis-à-vis du réseau ;

15 - il comporte des moyens pour gérer un profil d'informations basé sur des données personnelles et sur les communications qu'il établit avec le réseau ;

- il comporte des moyens pour protéger de la lecture par un fournisseur d'accès au réseau, au moins une partie des données échangées entre le serveur de protection et le terminal client ;

20 - il comporte des moyens pour dissimuler, au fournisseur d'accès, des adresses de sites hôtes à destination desquels sont envoyées des données, à partir du terminal client ;

25 - le serveur de protection fournit sur requête, à la place du fournisseur d'accès, une adresse de site hôte identifié par un nom, en correspondance de ce nom, à l'aide d'un système de nom de domaine ;

30 - il comporte des moyens pour éliminer une partie, comportant des informations sur l'identité du terminal client, d'une requête de connexion, formulée à partir du terminal client à destination d'un site hôte, avant que

cette requête transite vers le site hôte auquel elle est destinée ;

5 - il comporte une base de connaissances, associée à l'identité réelle de l'utilisateur ou à un avatar de l'utilisateur, dans laquelle sont enregistrées des informations sur le comportement de l'utilisateur lorsqu'il communique avec le réseau en utilisant respectivement son identité réelle ou cet avatar ;

10 - il comporte une base de données, destinée à stocker au moins un manifeste de la politique de protection des données personnelles d'un site hôte, et des moyens de comparaison de chaque manifeste avec les informations enregistrées dans la base de connaissances en association avec un avatar de l'utilisateur ou son identité réelle ; un tel manifeste est par exemple un formulaire P3P ; les moyens de comparaison sont avantageusement constitués d'un moteur d'inférence du statut de confiance ; un moteur d'inférence permet de produire de nouvelles propositions à partir de propositions tenues pour acquises, en mettant en oeuvre des 15 règles d'inférence ; dans l'ensemble serveur de protection, les propositions tenues pour acquises comprennent le manifeste de la politique de protection d'un site hôte, les nouvelles propositions comprennent le statut de confiance et les règles d'inférence sont définies à partir des 20 informations associées à l'avatar de l'utilisateur ;

25 - il comporte des moyens de filtrage de témoins en provenance du réseau et des moyens de stockage, après approbation par l'utilisateur, d'au moins une partie des témoins filtrés ;

30 - il comporte une pluralité de serveurs de protection organisés en un réseau de serveurs mandataires (aussi appelés « serveurs Proxy » par l'homme du métier)

pour permettre une plus grande proximité entre le terminal client et au moins l'un de ces serveurs de protection ;

5 - il comporte un serveur central pour diriger l'utilisateur vers le serveur de protection le plus proche du terminal client ; et

10 - il comporte un serveur dédié à la création d'avatars et au stockage de témoins, et comportant une base de connaissances, associée à l'identité réelle de l'utilisateur ou à un avatar, dans laquelle sont enregistrées des informations sur le comportement de l'utilisateur lorsqu'il communique avec le réseau en utilisant son identité réelle ou cet avatar.

15 Selon encore un autre aspect, l'invention propose un programme d'ordinateur chargeable dans une mémoire, associée à un processeur, et comprenant des portions de codes pour la mise en œuvre d'un procédé tel que mentionné précédemment, lors de l'exécution dudit programme.

20 Selon encore un autre aspect, l'invention propose un programme d'ordinateur chargeable dans une mémoire, associée à un processeur, et comprenant des portions de codes pour gérer la communication entre le terminal client et l'ensemble serveur de protection tel que mentionné précédemment, lors de l'exécution dudit programme.

25 Selon encore un autre aspect, l'invention propose un support de données sur lequel est enregistré un programme d'ordinateur tel que mentionné précédemment.

Selon encore un autre aspect, l'invention propose un procédé de téléchargement d'un programme d'ordinateur tel que mentionné précédemment.

30 D'autres aspects, buts et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit d'un de ses modes de réalisation. L'invention sera

également mieux comprise à l'aide des références aux dessins sur lesquels :

5 - la figure 1 représente, schématiquement, la structure de la communication entre un terminal client et un réseau de sites hôtes, dans un exemple de mode de mise en œuvre du procédé conforme à la présente invention ;

10 - la figure 2 représente, schématiquement, l'architecture d'un ensemble serveur pour la mise en œuvre de l'exemple de procédé représenté sur la figure 1 ; et

15 - la figure 3 représente, schématiquement, l'architecture des fonctions de protection de l'ensemble serveur dont l'architecture est représentée sur la figure 2.

15 L'invention est décrite ci-dessous dans le cadre de sa mise en œuvre pour confidentialiser la communication entre un terminal client, constitué d'un ordinateur personnel 1, et un ensemble de sites 2 hôtes tels que des sites Internet.

20 Comme représenté sur la figure 1, l'ordinateur personnel 1 est connecté à Internet via un fournisseur d'accès 3 et un ensemble serveur de protection 4.

L'ensemble serveur de protection 4 offre de nombreuses fonctions.

25 A titre illustratif, la figure 1 représente le cas où l'ensemble serveur de protection 4 permet, à l'internaute de l'ordinateur personnel 1 de contrôler et d'accepter ou non l'intervention de tiers lors de sa communication avec un site 2 destinataire. En effet, lorsqu'un utilisateur consulte une page sur ce site 2 destinataire, il peut arriver que cette page contienne des insertions émanant de tiers (publicité par exemple) et que, en outre, ce tiers 30 émette un cookie à destination de l'ordinateur de l'internaute. Grâce à l'ensemble serveur de protection 4

selon l'invention, l'internaute peut choisir d'accepter ou non le cookie émis par ce tiers.

L'architecture générale d'un ensemble serveur de protection 4 tel que celui représenté sur la figure 1 est 5 illustrée par la figure 2.

Cet ensemble serveur de protection 4 comporte principalement :

- un serveur d'Identification 5,
- un réseau de serveurs Mandataires 6, chaque 10 serveur Mandataire 6 étant associé à un serveur de Configuration, lui-même associé à un serveur de Connaissances Utilisateurs 8,
- un serveur de Services 9 et
- un serveur Superviseur 10.

15 Dans la suite de ce document, par souci de simplification, l'ensemble serveur de protection 4 est décrit avec un seul serveur Mandataire 6, auquel est associé un seul serveur de Configuration 7, lui-même associé à un seul serveur de Connaissances Utilisateurs 8, bien que ces 20 différents serveurs soient dupliqués en réseau.

25 Comme représenté sur cette figure 2, l'internaute accède au réseau Internet à partir de son ordinateur personnel 1. Afin d'utiliser les services de l'ensemble serveur de protection 4, l'internaute se sert d'outils d'accès, de configuration et de rapport.

Ces outils d'accès, de configuration et de rapport sont des programmes d'ordinateur 1 enregistrés dans la mémoire de l'ordinateur à partir d'un support tel qu'un cédérom ou après téléchargement à partir d'un site Internet 30 qui distribue de tels programmes.

Ces outils d'accès, de configuration et de rapport sont aptes à permettre à l'internaute :

- d'être identifié auprès de l'ensemble serveur de protection 4,

- de recevoir en retour un « jeton d'accès » pour une session,

5 - de créer des avatars ou modifier un avatar existant,

- de sélectionner un avatar pour se connecter au réseau Internet,

10 - de sélectionner un profil d'informations prédéfini, éventuellement de modifier ce profil d'informations prédéfini pour le personnaliser et/ou de créer complètement un profil d'informations,

- d'attacher à un avatar, le profil d'informations prédéfini sélectionné, modifié ou créé,

15 - de modifier un profil de préférence attaché à un avatar,

- d'obtenir un rapport de navigation,

20 - d'activer un service de protection de sa vie privée par l'ensemble serveur de protection 4 sur la base du profil d'information sélectionné et

- d'accéder à divers autres services accessibles sur l'ensemble serveur de protection 4.

25 L'internaute se connecte à l'ensemble serveur de protection 4, au niveau du serveur d'Identification 5. La fonction d'identification du serveur d'Identification est mise en œuvre grâce aux fonctions relatives au certificat d'identification personnel du navigateur Internet de l'internaute. Le serveur d'Identification confronte l'identité de l'internaute à des données sur les 30 utilisateurs ayant accès à l'ensemble serveur de protection 4, stockées dans une base de données Utilisateurs 11. Après

identification, les internautes autorisés reçoivent un "jeton d'accès" pour une session.

5 L'internaute ayant reçu un « jeton d'accès » à une session, accède au serveur Mandataire 6. Avantageusement et essentiellement pour des raisons de performances dans les vitesses de communication et de bandes passantes, le serveur Mandataire 6 est le serveur « Proxy » situé le plus proche possible de l'internaute.

10 Le serveur Mandataire 6 réalise l'interface entre l'internaute, les autres serveurs de l'ensemble serveur de protection 4 et le réseau Internet. Il a principalement pour fonctions de :

- filtrer et sélectionner les cookies en provenance du réseau ;

15 - effectuer une comparaison entre l'expression d'une politique de protection de la vie privée, d'un site 2 et le profil d'informations attaché à l'avatar utilisé par l'internaute pour accéder à ce site 2,

20 - dériver et stocker les cookies acceptés par l'internaute,

- modifier l'en-tête des requêtes de connexion,

25 - supprimer l'adresse d'identification (adresse IP) de l'internaute, des données envoyées aux sites 2 destinataires, ainsi que l'adresse de ces sites 2 destinataires, des données transitant par le fournisseur d'accès,

- remplir automatiquement des formulaires en fonction du statut de confiance associé au site 2 ayant émis ce formulaire

30 - faire, selon la table DNS, la conversion nom/adresse des sites 2 visés par l'internaute,

- analyser le contenu des pages Web consultées et retirer de ces pages les éléments non souhaités par l'internaute, et

5 - établir l'historique des sessions de connexion et les préférences de l'internaute.

Le filtrage et la sélection des cookies sont réalisés en fonction de données stockées dans une base de données d'Informations Utilisateurs 12 qui comporte entre autres choses, les souhaits de l'internaute quant au 10 traitement des cookies.

Les cookies considérés comme acceptables par l'internaute sont stockés dans une mémoire. Cette mémoire est accessible à l'internaute et au serveur du site 2 qui l'a émis, mais ne se situe pas sur l'ordinateur 1 de 15 l'internaute.

L'en-tête des requêtes de connexion, que cette connexion soit établie selon le protocole http ou selon un autre protocole, est modifiée, avant de transiter vers le site 2, en fonction de critères et de règles de protection 20 et de respect de la vie privée définies par des comités d'éthique.

L'historique des sessions et les préférences de l'internaute sont, selon son profil d'informations, soit détruites soit transférées au serveur de Connaissances 25 Utilisateurs 8 associé au serveur Mandataire 6.

Le serveur Mandataire 6 est programmé à l'aide de programmes libres et bien connus de l'homme du métier (Squid®, Apache®, etc.).

Le serveur de Configuration 5 permet de :

30 - créer, sélectionner ou modifier un avatar et/ou un profil d'informations,

- sélectionner, créer et/ou configurer des profils de préférences,

- consulter les cookies, les télécharger ou les détruire, et

5 - accéder à des services tels que « Aide », « FAQ », messagerie électronique, etc., ainsi qu'au rapport de navigation.

10 L'internaute a la possibilité de créer plusieurs avatars. A chaque avatar est attaché une ou plusieurs adresse(s) électronique(s), une mémoire de stockage de cookies et de fichiers de connexions, un profil d'informations, un profil de préférences, etc. Les profils d'informations et de préférences peuvent être différents d'un avatar à un autre.

15 Un profil d'informations comporte des informations identifiantes et des informations qualifiantes sur l'internaute. Les informations identifiantes sont, par exemple, son état civil, son adresse, etc. Les informations qualifiantes sont, par exemple, son âge, ses centres 20 d'intérêt, etc.. Les informations identifiantes peuvent être réelles ou virtuelles. Elles sont enregistrées pour chaque avatar. Le procédé selon l'invention en permet une divulgation contrôlée. L'internaute choisit de conférer un plus ou moins grand degré d'anonymat à un avatar donné. A 25 certains avatars, il peut associer un pseudonyme, tandis qu'il peut révéler son identité avec d'autres (par exemple pour des achats en ligne). Il peut aussi, par exemple, indiquer des centres d'intérêt différents selon les avatars pour obtenir des services personnalisés et spécialisés en 30 fonction de ces centres d'intérêt.

La gestion des profils d'informations, en relation avec les avatars de chaque internaute, est réalisée au

niveau du serveur de Connaissances Utilisateurs 8, grâce aux informations stockées dans la base de données d'Informations Utilisateurs 10. Le serveur de Connaissances Utilisateurs 8 et la base de données d'Informations Utilisateurs 10 sont 5 hautement sécurisés.

Cette gestion des profils d'informations est réalisée par l'internaute, grâce à une ou plusieurs page(s) Web éditée(s) et gérée(s) par le serveur de Configuration 7 en relation avec le serveur de Connaissances Utilisateurs 8. 10 Chaque page Web interface la communication entre l'internaute et ce serveur de Configuration 7.

A ces profils d'informations s'ajoutent un ou plusieurs profil(s) de préférences. Les profils de préférences de l'internaute sont générés à partir des 15 informations fournies directement par l'internaute ou à partir de l'analyse de son comportement (pages Web consultées, temps de connections, etc.). Un profil de préférences distinct peut être associé à chaque avatar. Les profils de préférences des utilisateurs sont stockées dans 20 une base de données Préférences Utilisateurs 13 directement accessible par le serveur de Configuration 7.

Le rapport de navigation comporte :
- l'historique des navigations de l'internaute,
- la liste des cookies reçus au cours de ces 25 navigations,

- l'état de la session de connexion en cours, qui informe en particulier l'internaute sur les profils attachés à l'avatar qu'il utilise et le ou les site(s) 2 au(x)quel(s) il est connecté,
30 - les récentes actions (par exemple : "Inactivation d'un cookie émis par 'Le serveur de bandeaux publicitaires X' lors de la consultation du site 'Les assurances Y'"), et

- des explications sur celles-ci (par exemple : « Le site hôte souhaitait accéder à l'historique de votre navigateur pour utiliser ces données en vue de la définition d'un profil et personnaliser ou adapter ses services à ce profil »).

L'état de la session de connexion en cours évolue avec le temps et est enregistré au fur à mesure de son évolution.

Le rapport de navigation est géré par le serveur de Connaissances Utilisateurs 8 via une interface générée par le serveur de Configuration 7. L'accès à cette interface se fait par l'intermédiaire du navigateur de l'internaute, grâce au « jeton d'accès ». Cet accès est lancé à partir d'une application spécifique telle qu'une icône ou une ligne de commande (Systray[®] pour un ordinateur fonctionnant avec Windows[®], Menu Bar Icon[®] sur un Mac[®], une icône sur une Linux[®] box).

Le serveur Mandataire 6 permet également d'accéder au serveur de Services 9.

Ce serveur de Services 9 gère, entre autres choses, des informations sur les sites hôtes et leur politique de protection de la vie privée des internautes. Ces informations sont utilisées dans la mise en œuvre des fonctions de protection de l'ensemble serveur de protection 4. L'ensemble des fonctions de protection est illustré par la figure 3.

Les fonctions de protection de l'ensemble serveur de protection 4 sont liées aux politiques d'utilisation des données personnelles par des sites 2 du réseau Internet, aux connaissances sur les menaces, vis à vis de la vie privée des internautes, que représentent certains des sites 2

(cookies de tiers, publicité, etc.) et à la messagerie électronique.

Plus précisément, les politiques d'utilisation des données personnelles par des sites 2 sont répertoriées et 5 stockées au niveau d'une base de données Politiques Protection 14. Ces politiques correspondent par exemple aux politiques P3P des sites 2 hôtes, avantageusement complétées par diverses informations. Ces diverses informations sur les sites 2 hôtes sont par exemple collectées par l'ensemble 10 serveur de protection 4 et stockées dans une base de données Connaissances Entreprises 15. Elles concernent par exemple l'utilisation des adresses électroniques faites par les sites 2, la réputation de ces sites 2 et les relations de ces sites 2 avec des sites tiers. La pérennité de ces 15 politiques et des informations auxquelles elles correspondent sont régulièrement contrôlées (par exemple avec un contrôle de type somme de contrôle).

A partir de la base de données Connaissances Entreprises 15, le serveur de Services :

20 - fournit des indications aux serveurs Mandataires 6 qui, complétées par les profils d'informations et de préférences, définissent le traitement automatique à opérer sur les flux de données échangées entre l'internaute et le réseau,

25 - établit des listes de domaines, d'adresses IP et autre sources d'informations susceptibles d'être utilisées par des serveurs de publicité et autres serveurs bien connus pour envoyer à destination des ordinateurs individuels, des cookies de traquage, et

30 - contrôle l'évolution de ces listes.

Les informations ainsi répertoriées, dans les bases de données Politiques Protection 14 et Connaissance

Entreprises 15, sont comparées au profil de préférences sélectionné dans la base de données Préférences Utilisateurs 13, par l'internaute pour inférer automatiquement un statut de confiance sur chaque site visité par l'internaute (voir 5 figure 3).

Le serveur de Services 9 gère également des messageries électroniques. Le serveur de Services 9 :

- fournit à la demande des adresses électroniques, à l'internaute utilisateur de l'ensemble serveur de protection

10 4,

- substitue des adresses à usage unique à de vraies adresses, par exemple après validation d'un formulaire proposé à l'internaute,

15 - effectue un suivi de l'utilisation des adresses à usage unique par les sites 2 auxquels elles sont destinées, analyse ce suivi et l'enregistre dans un journal,

- filtre les courriers électroniques entrants en fonction de leur provenance et des préférences de l'utilisateur,

20 - effectue éventuellement un contrôle anti-virus des courriers électroniques entrants et

- dispatche les courriers électroniques acceptés après le filtrage et le contrôle éventuels précédents.

25 Tous les serveurs de l'ensemble serveur de protection sont sous le contrôle du serveur Superviseur 10.

Ce serveur Superviseur 10 :

- gère la table DNS et dirige l'internaute, via un serveur central (non représenté), vers le serveur Mandataire 6 qui lui est le plus proche,

30 - fournit une interface pour des auditeurs et des fonctions de traçabilité sur requête de ces auditeurs, et

- surveille, en quasi temps réel, l'activité de chaque serveur de l'ensemble serveur de protection 4, avec enregistrement des événements dans un journal et contrôle des performances de l'ensemble serveur de protection 4.

5 Outre l'utilisation du réseau Internet en contrôlant la protection des données qui lui sont personnelles et la configuration d'outils de gestion de ce contrôle, l'ensemble serveur de protection 4 permet à un internaute autorisé d'accéder à d'autres Services tels que :

10 - la programmation d'alertes en fonction d'évènements dans des forums de discussion,
- l'interaction sécurisée avec des comptes bancaires, etc.

15 L'environnement relatif aux fonctions de communication avec le serveur de protection 4 et le réseau Internet est programmé en langage Java[®] ou PHP[®] (Hypertext Processor) .

REVENDICATIONS

1. Procédé de communication pour échanger de manière contrôlée des données entre un terminal client (1) et un réseau de sites (2) hôtes, ce procédé étant caractérisé par le fait que :

- les données sont échangées, entre le terminal client (1) et le réseau, par l'intermédiaire d'un serveur de protection (6),

10 - l'identifiant du terminal client est masqué, vis à vis du réseau, au niveau du serveur de protection (6),

15 - au moins une partie des données sont protégées de la lecture par toute personne non autorisée à lire cette partie des données, lorsque ces données sont communiquées entre le serveur de protection (6) et le terminal client (1),

- un profil de préférences qualifiant un utilisateur du terminal client et agréé par cet utilisateur est comparé à des connaissances sur au moins un site hôte (2), et

20 - l'échange des données entre le terminal client et ce site (2) hôte est contrôlé en fonction d'informations issues de cette comparaison.

25 2. Procédé selon la revendication 1, dans lequel l'utilisateur accède au serveur de protection (6) grâce à un fournisseur d'accès (3) au réseau, pour lequel les données échangées entre le serveur de protection (4) et le terminal client (1) sont au moins en partie protégées de la lecture.

30 3. Procédé selon la revendication 2, dans lequel des adresses de sites (2) hôtes à destination desquels sont envoyées des données, à partir du terminal client (1), sont dissimulées au fournisseur d'accès (3).

4. Procédé selon l'une des revendications 2 et 3, dans lequel le serveur de protection (6) fournit sur requête, à la place du fournisseur d'accès (3), une adresse de site hôte identifié par un nom, en correspondance de ce nom, à l'aide d'un système de nom de domaine.

5 5. Procédé selon l'une des revendications précédentes, dans lequel une partie, comportant des informations sur l'identité du terminal client (1), d'une requête formulée à partir du terminal client (1) à destination d'un site (2) hôte, est modifiée avant de transiter vers le site (2) hôte auquel est destinée la requête.

10 6. Procédé selon l'une des revendications précédentes, comprenant un filtrage de témoins en provenance du réseau par le serveur de protection (6) et un stockage, au niveau du serveur de protection (6), d'au moins une partie de ces témoins.

20 7. Procédé selon l'une des revendications précédentes, dans lequel un serveur de courrier électronique (9) fournit au moins une adresse de courrier électronique à usage unique.

25 8. Procédé selon la revendication 7, comprenant un suivi de l'utilisation de l'adresse à usage unique, faite par un tiers à qui cette adresse de courrier électronique a été transmise.

30 9. Procédé selon l'une des revendications précédentes, dans lequel une pluralité de comptes de messagerie électronique est attribuée à un utilisateur, avec un portail unique, indépendant du terminal client et personnel pour gérer ces comptes.

10. Procédé selon l'une des revendications précédentes, dans lequel un statut de confiance est associé

à un site (2) hôte, en fonction de connaissances, stockées dans une base de connaissances (14,15), sur au moins la politique de protection des données personnelles par un tiers exploitant ce site (2) hôte.

5 11. Procédé selon la revendication 10, dans lequel un formulaire de saisie d'informations sur l'utilisateur, fourni par un site (2) hôte et destiné à l'enregistrement des informations saisies, par ce site (2) hôte, est rempli automatiquement par le serveur de protection (6) en fonction du statut de confiance, avant d'être soumis à l'approbation de l'utilisateur.

10 12. Procédé selon la revendication 11, dans lequel l'approbation par l'utilisateur est réalisée automatiquement en fonction d'un profil de protection qu'il a prédefini.

15 13. Procédé selon l'une des revendications précédentes, dans lequel l'utilisateur du terminal client (1) est représenté, vis-à-vis du réseau, par au moins un avatar.

20 14. Procédé selon la revendication 13, dans lequel un profil d'informations comprenant le profil de préférences et associé à l'identité réelle de l'utilisateur ou à chaque avatar est stocké au niveau d'une base de connaissances (12,13), ce profil étant déterminé, au moins en partie, par le comportement de l'utilisateur lorsqu'il communique avec 25 le réseau en utilisant cet avatar.

15. Procédé selon la revendication 14, dans lequel le profil d'informations est modifié par l'utilisateur par l'intermédiaire d'un serveur de configuration (7).

30 16. Procédé selon l'une des revendications 13 à 15, dans lequel une autorisation d'utilisation, par un tiers exploitant un site (2) hôte, des informations attachées à l'identité réelle de l'utilisateur ou à l'avatar sous lequel

l'utilisateur accède à ce site (2) hôte est régie par l'utilisateur, au moyen de la sélection et de l'activation d'un profil de protection prédefini.

17. Procédé selon les revendications 10 et 16 prises 5 en combinaison, dans lequel le profil de protection est confronté au statut de confiance pour définir un traitement automatique des données échangées entre ce site (2) hôte et le terminal client (1), lorsque l'utilisateur souhaite établir une communication avec un site (2) hôte et 10 préalablement à cette communication, et lorsqu'un site hôte (2) souhaite entrer en communication avec le terminal client.

18. Procédé selon les revendications 6 et 17 prises 15 en combinaison, dans lequel le traitement automatique des données échangées entre le site (2) hôte et le terminal client (1) comporte le filtrage de témoins en provenance du réseau et le stockage, au niveau du serveur de protection (6), d'au moins une partie des témoins filtrés.

19. Ensemble serveur de protection pour faire 20 l'interface entre un terminal client (1) et un réseau de sites (2) hôtes et permettre à un utilisateur du terminal client de contrôler la diffusion d'informations qui le concernent, sur le réseau, cet ensemble serveur de protection (6) comportant :

25 - des moyens, au niveau d'un serveur de protection (6), pour masquer l'identifiant du terminal client, vis à vis du réseau,

30 - des moyens pour protéger au moins une partie des données, de la lecture par toute personne non autorisée à lire cette partie des données, lorsque ces données sont communiquées entre le serveur de protection (6) et le terminal client (1),

- des moyens de comparaison pour comparer, à des connaissances sur au moins un site hôte (2), un profil de préférences qualifiant l'utilisateur et agréé par ce dernier, et

5 - des moyens pour contrôler, en fonction d'informations générées par les moyens de comparaison, l'échange des données entre le terminal client et ce site (2) hôte.

10 20. Ensemble serveur de protection selon la revendication 19 comportant des moyens (8) pour créer au moins un avatar permettant de représenter l'utilisateur vis à vis du réseau.

15 21. Ensemble serveur de protection selon l'une des revendications 19 et 20, comportant des moyens pour gérer un profil d'informations basé sur des données personnelles et sur les communications qu'il établit avec le réseau.

20 22. Ensemble serveur de protection selon l'une des revendications 19 à 21, comportant des moyens pour protéger de la lecture par un fournisseur d'accès au réseau (3), au moins une partie des données échangées entre le serveur de protection (6) et le terminal client (1).

25 23. Ensemble serveur de protection selon la revendication 22, comportant des moyens pour dissimuler, au fournisseur d'accès (3), des adresses de sites (2) hôtes à destination desquels sont envoyées des données, à partir du terminal client (1).

30 24. Ensemble serveur de protection selon l'une des revendications 22 et 23, dans lequel le serveur de protection (6) fournit sur requête, à la place du fournisseur d'accès (3), une adresse de site (2) hôte identifié par un nom, en correspondance de ce nom, à l'aide d'un système de nom de domaine.

25. Ensemble serveur de protection selon l'une des revendications 19 à 24, comportant des moyens pour éliminer une partie, comportant des informations sur l'identité du terminal client (1), d'une requête de connexion, formulée à 5 partir du terminal client (1) à destination d'un site (2) hôte, avant que cette requête transite vers le site (2) hôte auquel elle est destinée.

26. Ensemble serveur de protection selon l'une des revendications 20 à 25, comportant une base de connaissances 10 (13), associée à l'identité réelle de l'utilisateur ou à un avatar de l'utilisateur, dans laquelle sont enregistrées des informations sur le comportement de l'utilisateur lorsqu'il communique avec le réseau en utilisant respectivement son identité réelle ou cet avatar.

15 27. Ensemble serveur de protection selon la revendication 26, comportant :

- une base de données (14,15) destinée à stocker au moins un manifeste de la politique de protection des données personnelles d'un site (2) hôte, et

20 - des moyens de comparaison de chaque manifeste avec les informations enregistrées dans la base de connaissances (12,13) en association avec un avatar de l'utilisateur ou son identité réelle.

25 28. Ensemble serveur de protection selon l'une des revendications 19 à 27, comportant des moyens de filtrage de témoins en provenance du réseau et des moyens de stockage, après approbation par l'utilisateur, d'au moins une partie des témoins filtrés.

30 29. Ensemble serveur de protection selon l'une des revendications 19 à 28, comportant une pluralité de serveurs de protection (6) organisés en un réseau de serveurs mandataires pour permettre une plus grande proximité entre

le terminal client (1) et au moins l'un de ces serveurs de protection (6).

30. Ensemble serveur de protection selon la revendication 29, comportant un serveur central pour diriger 5 l'utilisateur vers le serveur de protection (6) le plus proche du terminal client (1).

31. Ensemble serveur de protection selon l'une des revendications 19 à 30, comportant un serveur (8) dédié à la création d'avatars et au stockage de témoins, et comportant 10 une base de connaissances (13), associée à l'identité réelle de l'utilisateur ou à un avatar, dans laquelle sont enregistrées des informations sur le comportement de l'utilisateur lorsqu'il communique avec le réseau en utilisant respectivement son identité réelle ou cet avatar.

15 32. Programme d'ordinateur chargeable dans une mémoire, associée à un processeur, et comprenant des portions de codes pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 18, lors de l'exécution dudit programme.

20 33. Programme d'ordinateur chargeable dans une mémoire, associée à un processeur, et comprenant des portions de codes pour gérer la communication entre le terminal client (1) et l'ensemble serveur de protection (6) selon l'une des revendications 19 à 31, lors de l'exécution 25 dudit programme.

34. Support de données sur lequel est enregistré un programme d'ordinateur selon l'une des revendications 32 et 33.

30 35. Procédé de téléchargement d'un programme d'ordinateur selon l'une des revendications 32 et 33.

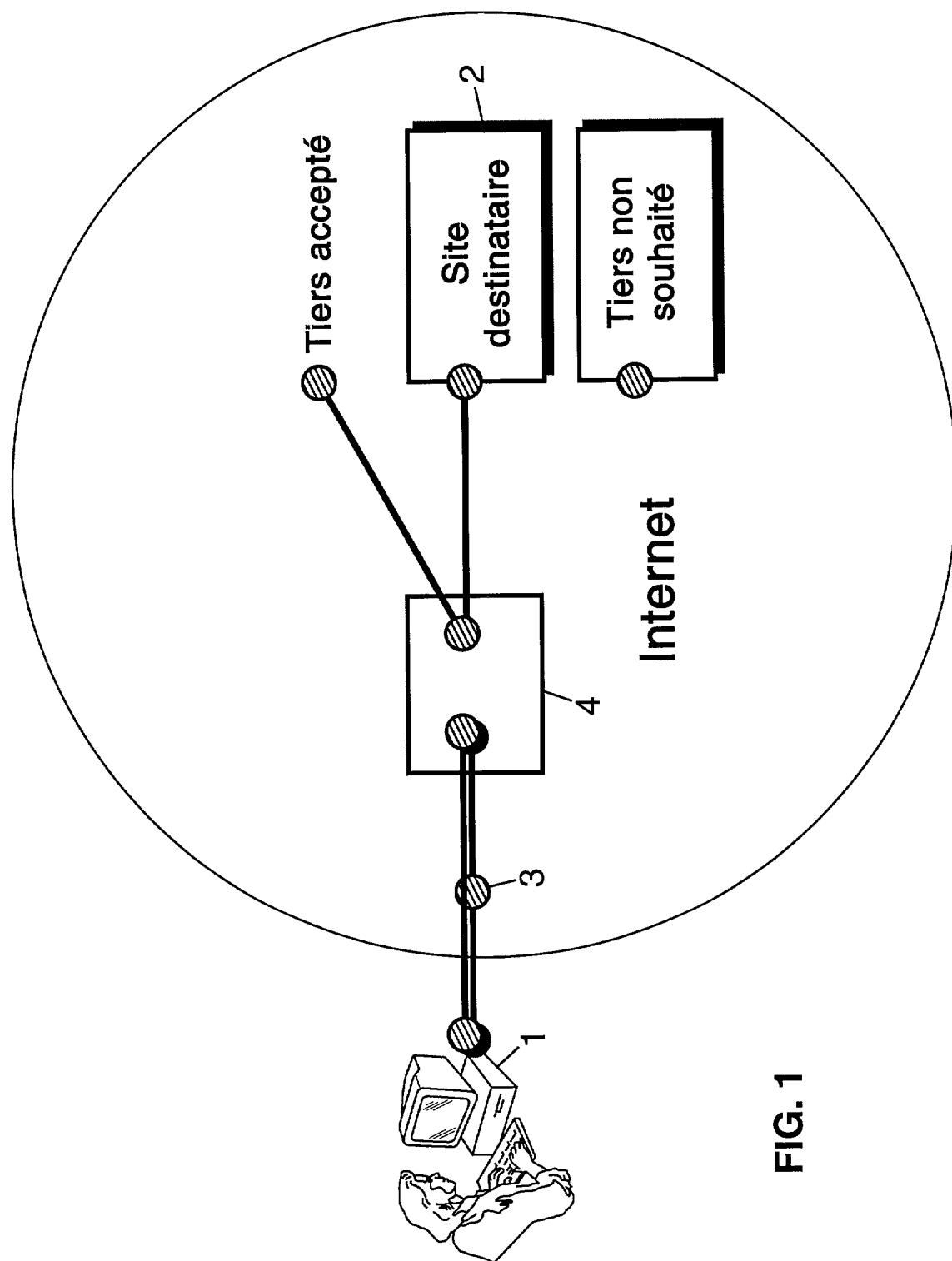
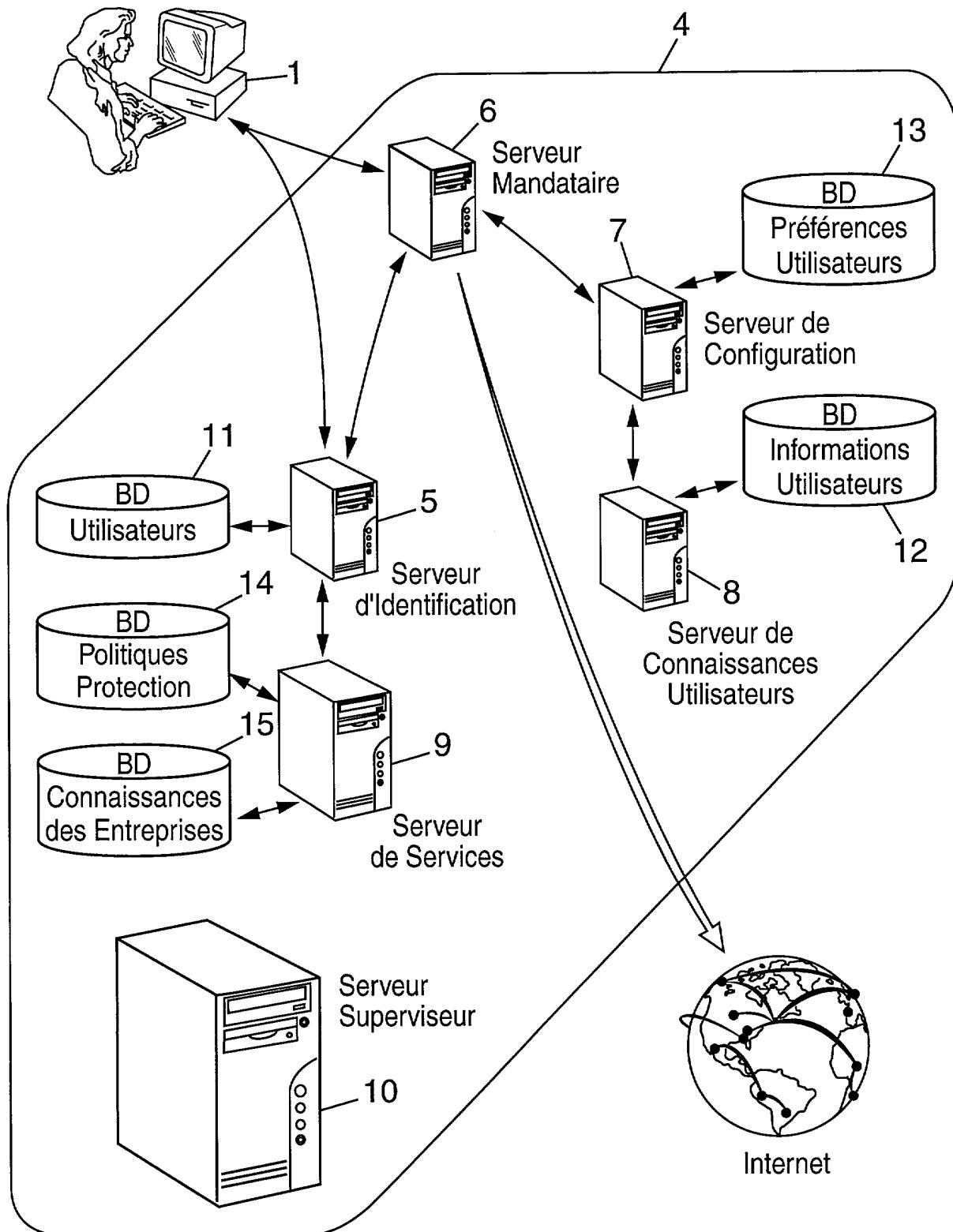
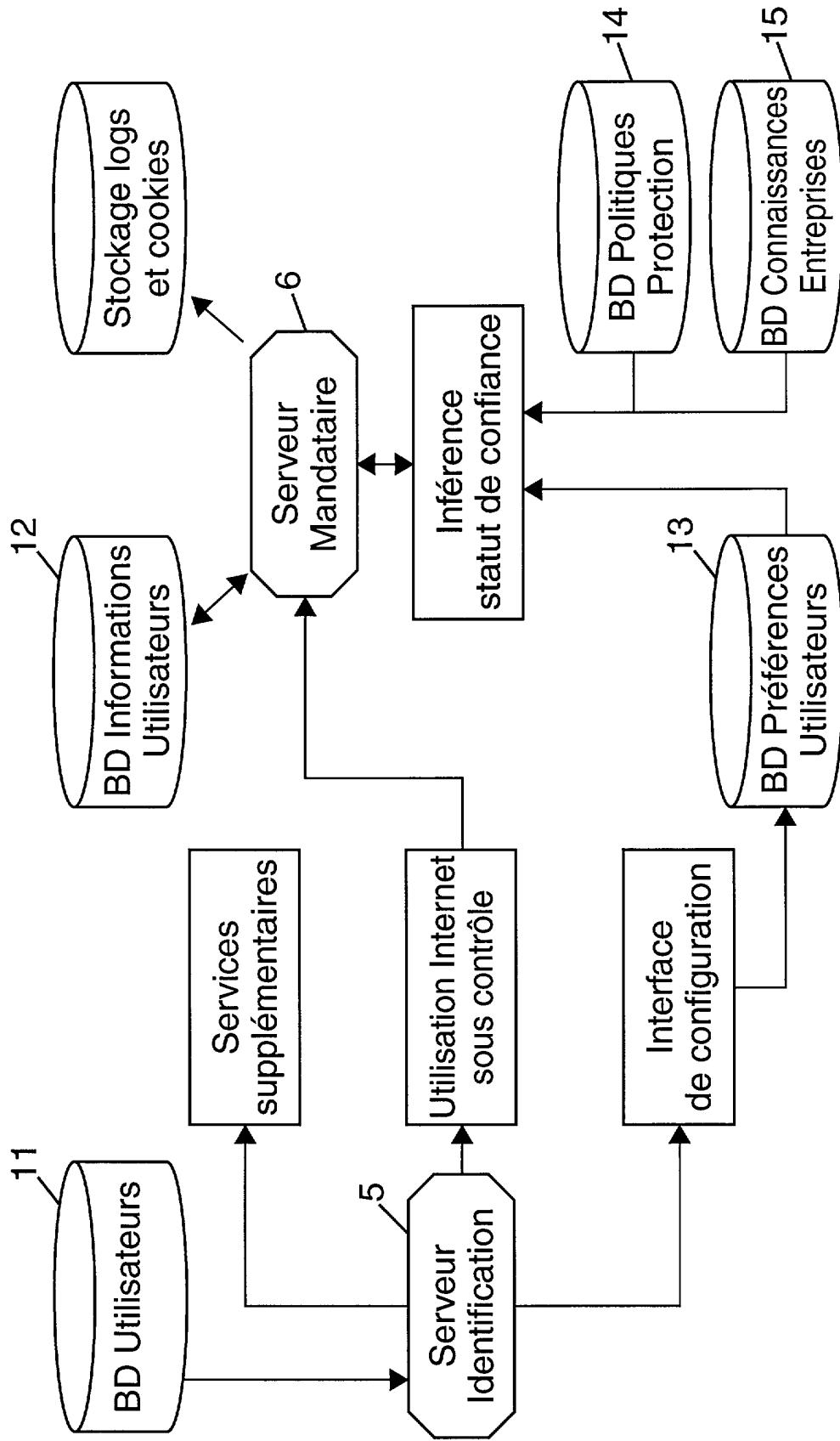


FIG. 1

**FIG. 2**

**FIG. 3**

RAPPORT DE RECHERCHE
PRÉLIMINAIRE

2828362

N° d'enregistrement
national

FA 606720
FR 0110413

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

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 01 50299 A (LEVY RAN ;SHAI AVI (IL); PANGO SYSTEMS B V (NL); PALGI BOAZ (NL)) 12 juillet 2001 (2001-07-12) * abrégé * * page 3, ligne 29 – page 6, ligne 29 * ----	1-35	H04L29/06 H04L12/22
A	EP 0 951 158 A (CITICORP DEV CENTER INC) 20 octobre 1999 (1999-10-20) * abrégé * * page 3, colonne 4, ligne 22 – page 4, colonne 6, ligne 8 * * page 5, colonne 7, ligne 19 – ligne 38 * ----	1-35	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L
1	Date d'achèvement de la recherche	Examinateur	
	28 mai 2002	Adkhis, F	
CATÉGORIE DES DOCUMENTS CITÉS		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	
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0110413 FA 606720**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **28-05-2002**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)	Date de publication
WO 0150299	A	12-07-2001	AU WO	1882501 A 0150299 A2	16-07-2001 12-07-2001
EP 0951158	A	20-10-1999	US AU AU BR CN EP EP EP EP EP EP JP JP JP JP JP SG SG TW WO WO US	2002004783 A1 1584499 A 1796599 A 9806416 A 1233804 A 0917119 A2 0917120 A2 0951158 A2 0950992 A2 0950972 A2 2000036049 A 2000076189 A 2000251006 A 11250165 A 11232348 A 78323 A1 76609 A1 381241 B 9924891 A2 9924892 A2 2001011250 A1	10-01-2002 31-05-1999 31-05-1999 16-11-1999 03-11-1999 19-05-1999 19-05-1999 20-10-1999 20-10-1999 20-10-1999 02-02-2000 14-03-2000 14-09-2000 17-09-1999 27-08-1999 20-02-2001 21-11-2000 01-02-2000 20-05-1999 20-05-1999 02-08-2001