(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 803 461**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 17147**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 F 19/00 // G 06 F 159:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.12.00.

(30) **Priorité :** 31.12.99 US 09477041.

(43) **Date de mise à la disposition du public de la demande :** 06.07.01 Bulletin 01/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

(71) **Demandeur(s) :** *GE MEDICAL TECHNOLOGY SERVICES, INC.* — US.

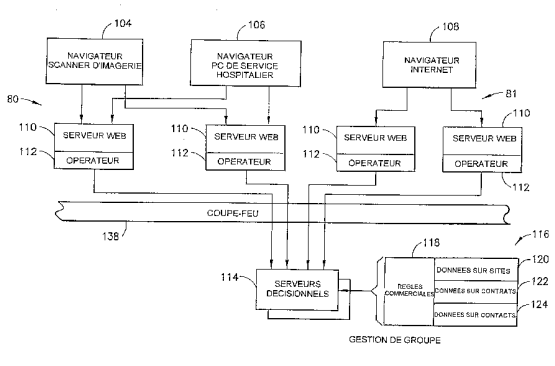
(72) **Inventeur(s) :** HUMMEL HENRY JOHN JR, SINGH KARAMJEET, LAMOUREAUX THOMAS LEROY, ZETTEL HUBERT ANTHONY, KELLY MICHAEL EVAN, PLOETZ LAWRENCE EDWARD, MEHRING DAVID THOMAS et PALLIYAL SUNIL MELEPATT.

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

(74) **Mandataire(s) :** CASALONGA ET JOSSE.

(54) PROCEDE ET DISPOSITIF POUR LA GESTION DE GROUPES DANS L'ENTRETIEN DE SERVICES DISTANTS.

(57) Procédé et système pour fournir des applications logicielles protégées à des systèmes distants à partir d'une structure centrale de services, la fourniture étant gérée sur la base de l'appartenance de l'utilisateur de système distant à un groupe. Des règles commerciales (118) servent à déterminer si un utilisateur particulier authentifié cherchant à accéder à une application logicielle protégée depuis un site distant particulier doit être autorisé. Une multitude de serveurs Web (110) sont programmés pour autoriser un accès sélectif à une ou plusieurs applications logicielles résidentes pour des utilisateurs de systèmes distants, par l'intermédiaire d'un réseau (80). L'accès est géré par un serveur décisionnel central (114) sur la base d'informations relatives à l'utilisateur et au système et de définitions de groupes stockées dans une base de données. Le serveur décisionnel communique avec chaque serveur Web à l'aide d'un module intermédiaire (112) qui fait partie du serveur Web. Le module intermédiaire intercepte les demandes d'accès émanant d'utilisateurs de systèmes distants, puis entre en liaison avec le serveur décisionnel. Si l'utilisateur de système distant a entré un code d'identification authentique, le serveur décisionnel applique alors les règles commerciales pour déterminer si l'utilisateur de système distant qui a fait la demande est autorisé à accéder au logiciel protégé demandé.



FR 2 803 461 - A1

Procédé et dispositif pour la gestion de groupes dans l'entretien de services distants

La présente invention est relative, d'une manière générale, à la protection des logiciels et au contrôle de la licence d'utilisation d'un logiciel d'application et de fichiers de données pour des applications à distance.

Le contrôle à distance et le télédiagnostic d'équipements ou de systèmes constituent un exemple d'application à distance. Actuellement, de nombreuses entreprises élaborent des moyens pour le contrôle à distance et le télédiagnostic d'équipements ou de systèmes. Les équipements ou systèmes distants (ci-après appelés systèmes distants) couvrent une gamme s'étendant des turbines à vapeur industrielles aux imprimantes en réseau, des équipements d'imagerie médicale à l'électroménager. Dans presque tous les cas, il existe dans les systèmes distants un moyen informatique tel qu'un processeur. Généralement, le processeur assure des fonctions telles que la collecte de données, le contrôle du fonctionnement, l'exécution d'applications diagnostiques et l'accès de l'utilisateur final ou du client à des informations et des applications dans les systèmes distants.

Dans une application typique du contrôle à distance, le logiciel et d'autres fichiers de données résidant dans un système distant échappent au contrôle direct du fournisseur, car ils se trouvent dans l'environnement du client. Cependant, certaines des applications logicielles et certains des fichiers de données présents dans cet environnement informatique contiennent beaucoup d'informations confidentielles et nécessitent une protection contre les accès non autorisés (par exemple aboutissant à une modification involontaire ou motivée par une volonté de vandalisme). L'accès non autorisé aux applications logicielles ou aux fichiers de données tels que les fichiers de configuration résidant dans le système distant risque d'empêcher un utilisateur d'avoir

accès à une fonction nécessaire. Selon une autre possibilité, l'accès non autorisé risque de permettre à un utilisateur d'accéder à une fonction réservée. Il est même possible que ces viols aboutissent à des pannes d'équipements

Par conséquent, on connaît des systèmes pour protéger contre le viol informatique des applications logicielles et des fichiers de données de configuration résidant dans un système distant. Un premier système connu utilise des mécanismes permettant d'assurer que des fichiers sont inaccessibles pour un client qui n'a pas payé pour ceux-ci et auxquels l'accès a été résilié. Ces mécanismes assurent également que des moyens diagnostiques ne sont pas accessibles à des prestataires de services autres que des fournisseurs susceptibles d'intervenir sur le système distant.

D'une manière typique, des techniciens d'entretien habilités procèdent à des appels de services en direction des sites distants dans le but d'intervenir sur les équipements présents sur ces sites. Lorsqu'il est sur site, le technicien d'entretien peut communiquer avec une structure centrale de services par l'intermédiaire d'un réseau utilisant une unité de services d'entretien. L'unité de services d'entretien peut comprendre un ordinateur portable conçu pour être utilisé sur des sites distants par des techniciens d'entretien. L'unité comprend une plate-forme de services qui comporte certains circuits correspondant à des fonctions pour établir une base de services uniforme pour les systèmes distants. De plus, les unités de services comprennent des outils de services spécifiques permettant au technicien d'entretien de demander et de recevoir des messages de services distants, des rapports sur des systèmes spécifiques d'établissement de diagnostics, des calendriers d'interventions, etc. Par l'intermédiaire de la plate-forme de services, le technicien d'entretien peut accéder à des configurations de systèmes, des informations d'archives, des informations sur un réseau de systèmes, des journaux et des données d'analyses, etc. Le technicien d'entretien peut également actualiser des fiches d'interventions. D'une manière typique, l'unité de services d'entretien est programmée avec un module d'accès pour permettre à la structure de services de vérifier les conditions de licence d'utilisation et de sécurité de l'unité de services d'entretien. Par exemple, le module d'accès, en coopération avec des circuits dans la structure de services, peut permettre à un technicien d'entretien d'accéder à des données ou à des applications assurant certaines ou la totalité des fonctions offertes aux techniciens d'entretien dans la structure de services. Ces fonctions peuvent être semblables à celles assurées dans les systèmes distants eux-mêmes, ou peuvent proposer aux techniciens d'entretien un choix plus large de services. En particulier, l'unité de services d'entretien peut être équipée d'applications de services, par exemple pour

analyser des données de fonctionnement d'un système d'établissement de diagnostics, programmer des appels de services réguliers ou spéciaux, planifier l'expédition ou le remplacement de pièces, etc. D'autres applications peuvent permettre au technicien d'entretien d'adresser des demandes de services à partir du système distant et d'émettre des messages de services et des actualisations par l'intermédiaire de l'unité de services d'entretien. les unités de services d'entretien peuvent être constituées par des ordinateurs personnels ou des ordinateurs portables de n'importe quelle plate-forme de traitement appropriée.

Evidemment, les techniciens d'entretien habilités ont besoin d'accéder à des applications logicielles différentes de celles auxquelles accèdent d'autres utilisateurs du système. En particulier, le technicien d'entretien a besoin d'accéder à un logiciel exclusif et extrêmement confidentiel sous la forme d'outils de services, de documentations de services et de fiches de services pour permettre d'apporter une solution aux problèmes concernant les systèmes et une remise en état adéquate des équipements. Il va de l'intérêt commercial de l'exploitant de la structure centrale de services que l'accès à un logiciel particulier et très confidentiel soit limité aux personnes autorisées, c'est-à-dire aux personnes ayant le niveau d'habilitation requis. De préférence, le système de sécurité doit permettre au personnel d'entretien et aux autres personnes habilitées d'accéder au logiciel central de nature très confidentielle depuis le système distant sur lequel une intervention est en cours tout en empêchant d'autres utilisateurs autorisés qui n'ont pas le niveau d'habilitation nécessaire d'accéder à ce logiciel.

On a donc besoin d'un système pour assurer toutes sortes d'applications logicielles à des groupes très divers d'utilisateurs de systèmes distants sur la base de niveaux de sécurité différents. Dans le cas où une entité commerciale telle qu'un hôpital a passé un contrat d'entretien avec un fournisseur qui assure des services sur site et un accès à des sites distants pour des applications logicielles résidant dans une structure centrale, on a besoin d'un procédé de gestion d'accès à distance à ce logiciel par des utilisateurs ayant des niveaux d'habilitation différents. Le système doit également pouvoir assurer des droits d'accès différents à des personnes différentes ayant le même niveau d'habilitation. Par exemple, à chaque niveau d'habilitation, une distinction supplémentaire doit être faite entre les utilisateurs sur la base des différents niveaux d'habilitation et des différentes responsabilités professionnelles (c'est-à-dire de l'appartenance à des groupes différents), qui entraînent la nécessité d'accéder à des applications logicielles différentes nécessitant un niveau de sécurité particulier.

L'invention concerne un procédé et un système pour fournir des applications logicielles protégées à des systèmes distants à partir d'une structure centrale de services, la fourniture étant gérée sur la base du niveau d'habilitation et sur la base de l'appartenance de l'utilisateur de systèmes distants à un groupe. Un principe de sécurité reposant sur un seul facteur est utilisé pour déterminer si des utilisateurs de systèmes distants cherchant à accéder à des applications logicielles à faible niveau de protection sont bien des utilisateurs autorisés. Des règles commerciales sont utilisées pour déterminer si les utilisateurs authentifiés qui désirent un accès doivent être autorisés.

Selon les formes préférées de réalisation de l'invention, une multitude de serveurs Web sont programmés pour permettre un accès sélectif à une ou plusieurs applications logicielles résidentes pour des utilisateurs de systèmes distants, par l'intermédiaire d'un réseau. Certaines applications sont libres et d'autres sont protégées, deux niveaux de protection étant de préférence mis en œuvre. L'accès est géré par un serveur décisionnel central sur la base d'informations relatives aux utilisateurs et aux systèmes et de définitions de groupes stockées dans une base de données. Le serveur décisionnel communique avec chaque serveur Web grâce à un module intermédiaire intégré dans le serveur Web.

Le module intermédiaire intercepte les demandes d'accès émanant d'utilisateurs de systèmes distants et établit une connexion avec le serveur décisionnel. Le module intermédiaire détermine si l'application demandée est libre ou protégée. Si l'application logicielle demandée est libre, le module intermédiaire demande au serveur Web d'autoriser l'accès. Si l'application logicielle demandée est protégée, le module intermédiaire prend contact avec le serveur décisionnel. Le serveur décisionnel authentifie des mots de passe, tout en rapportant à un serveur de sécurité l'authentification des codes de sécurité correspondants. Pour des applications logicielles à faible niveau de sécurité, si le mot de passe est authentifié, le serveur décisionnel applique alors les règles commerciales pour déterminer si l'utilisateur de système distant qui fait la demande est autorisé à accéder à l'application logicielle protégée. Un particulier peut être simultanément membre de groupes différents.

Selon la forme préférée de réalisation de l'invention, différents algorithmes d'authentification d'utilisateurs sont employés selon que l'utilisateur a un niveau d'habilitation à un seul facteur ou à deux facteurs. Les utilisateurs à niveau d'habilitation à un seul facteur sont en droit d'accéder à des applications logicielles à faible niveau de protection, tandis que ceux à niveau d'habilitation à deux facteurs sont

en droit d'accéder à des applications logicielles à la fois à faible niveau de protection et à haut niveau de protection. De préférence, l'utilisateur d'un système distant particulier envoie une demande d'accès à une application logicielle particulière à l'aide d'un navigateur Web situé dans le système distant, ce dernier étant connecté par un réseau au serveur Web où réside l'application logicielle demandée. Si l'utilisateur a un niveau d'habilitation à deux facteurs, pendant l'ouverture de session il doit entrer les deux facteurs, par exemple un mot de passe et un code de sécurité, en plus d'une identification d'utilisateur. Si l'utilisateur a seulement un niveau d'habilitation à un facteur, seul ce facteur unique (par exemple un mot de passe) et l'identification d'utilisateur sont entrés pendant d'ouverture de session.

Dans les deux cas, le module intermédiaire pour le serveur Web où réside le logiciel demandé intercepte la demande d'accès et les informations fournies par l'utilisateur dans le cadre de l'ouverture de session, puis il les transmet au serveur décisionnel central. De préférence, les serveurs Web répartis sont séparés du serveur décisionnel central par un coupe-feu. Les informations transmises sont traitées par le serveur décisionnel pour déterminer si la demande d'accès doit être acceptée. Ce traitement comprend deux étapes : (1) authentification de l'utilisateur ; et (2) autorisation d'accès à l'application logicielle demandée. Le serveur décisionnel authentifie le mot de passe en consultant une base de données de gestion de groupes accessible de manière électronique. Pour accéder aux applications logicielles à faible niveau de sécurité, si le mot de passe est authentique, le serveur décisionnel poursuit alors pour déterminer si l'accès doit être autorisé sur la base de l'utilisateur, du site, du système, d'un contrat et d'autres informations et règles commerciales (c'est-à-dire des définitions de groupes) dans la base de données de gestion de groupes. Les règles commerciales appliquent certains critères pour déterminer si le groupe particulier auquel appartient l'utilisateur est autorisé à accéder aux applications logicielles protégées demandées.

L'invention et nombre des avantages qui s'y attachent apparaîtront facilement plus clairement en référence à la description détaillée ci-après, faite en considération des dessins annexés, sur lesquels :

la Fig. 1 est une représentation schématique d'une série de systèmes d'établissement de diagnostics médicaux couplés à une structure de services par l'intermédiaire d'une connexion en réseau pour fournir des services et des échanges de

données d'une manière centralisée entre les systèmes d'établissement de diagnostics et la structure de services ;

la Fig. 2 est un schéma de principe des systèmes représentés sur la Fig. 1, illustrant certains organes des systèmes d'établissement de diagnostics et de la structure de services ;

la Fig. 3 est un schéma de principe représentant les organes d'une plate-forme de services uniforme utilisable dans un système distant ;

la Fig. 4 est un schéma de principe représentant des parties d'un système de gestion de groupes selon la forme préférée de réalisation de l'invention ;

la Fig. 5 est un schéma de principe représentant des parties d'un système de gestion d'accès distant pour un groupe à niveau d'habilitation selon la forme préférée de réalisation de l'invention ;

la Fig. 6 est un organigramme représentant globalement le processus de gestion de groupes à habilitation selon la forme préférée de réalisation de l'invention ;

la Fig. 7 est un schéma de principe représentant un système hybride qui combine la forme préférée de réalisation de l'invention avec le système classique illustré sur les figures 1 et 2.

La description détaillée ci-après de la forme préférée de réalisation de l'invention est présentée dans le contexte d'une structure centrale pour l'entretien d'une multitude de systèmes distants d'établissement de diagnostics médicaux et de postes de travail, par l'intermédiaire d'un réseau. Cependant, il doit être entendu que l'invention est applicable dans n'importe quel système où des systèmes distants utilisent des fichiers sous licence de logiciels et/ou de bases de données et sont connectés à une structure centrale par l'intermédiaire d'un réseau.

En référence à la Fig. 1, il est représenté un système 10 de services selon la technique antérieure, servant à assurer un service centralisé pour une pluralité de systèmes distants d'établissement de diagnostics médicaux 12. Dans la forme de réalisation représentée sur la Fig. 1, les systèmes d'établissement de diagnostics médicaux comprennent un système 14 d'imagerie par résonance magnétique nucléaire (RMN), un système 16 de tomographie (CT) assistée par ordinateur et un système 18 d'imagerie par ultrasons. Les systèmes d'établissement de diagnostics peuvent être installés à un seul endroit ou dans un seul établissement tel qu'un établissement médical 20, ou peuvent être distants les uns des autres comme représenté dans le cas du système 18 à ultrasons. Les interventions sur les systèmes d'établissement de diagnostics sont

effectuées à partir d'une structure centralisée 22 de services. En outre, une pluralité d'unités d'entretien 24 peuvent être couplées dans le système de services pour transmettre des demandes de services, vérifier le déroulement d'un service, transmettre des données de services, etc., comme décrit plus en détail ci-après.

Selon le mode de fonctionnement des systèmes, divers organes secondaires ou systèmes secondaires seront présents. Dans le cas du système 14 d'IRM, de tels systèmes comprendront généralement un scanner 26 servant à générer des champs magnétiques pulsés et à collecter des signaux résultant d'émissions par une substance gyromagnétique chez un sujet examiné. Le scanner est couplé à un circuit 28 de commande et de détection de signal qui est lui-même couplé à un dispositif de commande 30 du système. Le dispositif de commande 30 du système comprend une plate-forme uniforme servant à réaliser un échange interactif de demandes de services, de messages et de données avec la structure de services 22, comme décrit plus en détail ci-après. Le dispositif de commande 30 du système est relié à un module de transmission 32 qui peut faire partie du même ensemble physique que le dispositif de commande 30 du système ou d'un ensemble physique séparé. Le dispositif de commande 30 du système est également relié à un poste 34 d'opérateur qui comportera d'une manière typique un écran 36 d'ordinateur, un clavier 38 ainsi que d'autres dispositifs de saisie 40, par exemple une souris. Dans un système typique, des organes supplémentaires peuvent faire partie du système 14, par exemple une imprimante ou un système photographique servant à réaliser des images reconstruites à partir de données recueillies à l'aide du scanner 14.

De même, le système 16 de CT comprendra d'une manière typique un scanner 42 détectant des parties d'un rayonnement X dirigé à travers un sujet examiné. Le scanner 42 est couplé à un générateur et un dispositif de commande, ainsi qu'à une unité d'acquisition de signaux, l'ensemble étant désigné collectivement sous le repère 44, servant à commander le fonctionnement d'une source de rayons X et d'un portique de radiographie dans le scanner 42, et pour recevoir des signaux produits par une série de détecteurs mobiles à l'intérieur du scanner. Les circuits présents dans le dispositif de commande et les organes d'acquisition de signaux sont couplés à un dispositif de commande 46 du système qui, comme le dispositif de commande 30 évoqué plus haut, comprend des circuits pour commander le fonctionnement du scanner et pour traiter et reconstruire des données d'images sur la base des signaux acquis. Le dispositif de commande 46 du système est relié à un module de transmission 48, globalement semblable au module de transmission 32 du système 14 d'IRM, pour émettre et recevoir

des données pour le service central du système 16. Par ailleurs, le dispositif de commande 46 du système est couplé à un poste 50 d'opérateur qui comprend un écran 52 d'ordinateur, un clavier 54, ainsi que d'autres dispositifs de saisie 56 tels qu'une souris. De plus, comme le système 14 d'IRM, le système 16 de CT comprendra généralement une imprimante ou autre dispositif similaire pour sortir des images reconstruites sur la base de données recueillies par le scanner 42.

Les autres dispositifs de fonctionnement comprennent des circuits et du matériel à configuration particulière pour l'acquisition ou la production de signaux en fonction de leur conception particulière. En particulier, le système 18 d'imagerie par ultrasons comprendra globalement un scanner et une unité de traitement 58 de données servant à émettre des ultrasons vers un sujet examiné, et pour acquérir de la sorte des signaux qui sont traités pour reconstruire une image utile. Le système comprend un dispositif de commande 60 de système qui régule le fonctionnement du scanner 58 et qui traite les signaux acquis pour reconstruire l'image. De plus, le système 18 comprend un module de transmission 62 servant à transmettre des demandes de services, des messages et des données entre le dispositif de commande 60 du système et la structure de services 22. Le système 18 comprend également un poste 64 d'opérateur comportant un écran 66 ainsi que des dispositifs de saisie tels qu'un clavier 68.

S'il y a plusieurs systèmes d'établissement de diagnostics médicaux dans une seule structure ou à un seul endroit, comme indiqué dans le cas des systèmes d'IRM et de CT 14 et 16 de la Fig. 1, ceux-ci peuvent être couplés à un poste de gestion 70, tel que celui existant dans un service de radiologie d'un hôpital ou d'une clinique. Le poste de gestion peut être relié directement à des dispositifs de commande pour les divers systèmes d'établissement de diagnostics, par exemple les dispositifs de commande 30 et 46 dans l'exemple illustré. Le système de gestion peut comporter un poste de travail en informatique ou un ordinateur personnel 72 couplé aux dispositifs de commande du système sous une configuration Intranet, une configuration de partage de fichiers, une architecture client-serveur ou toute autre architecture appropriée. Le poste de gestion 70 comprendra d'une manière typique un écran 74 permettant de visualiser des paramètres de fonctionnement du système, d'analyser l'utilisation du système et d'échanger des demandes de services et des données entre la structure distante 20 et la structure centrale 22 de services. Des dispositifs de saisie tels qu'un clavier 76 d'ordinateur classique et une souris 78 peuvent également être prévus pour faciliter le dialogue pour l'utilisateur. Il faut souligner que, selon une autre possibilité, le système de gestion ou d'autres éléments d'un système d'établissement de diagnostics peuvent être

autonomes, c'est-à-dire qu'ils peuvent ne pas être couplés directement à un système d'établissement de diagnostics. Dans de tels cas, la plate-forme de service décrite ici, et une partie ou la totalité des fonctions de services peuvent néanmoins être assurées dans le système de gestion. De même, dans certaines applications, un système d'établissement de diagnostics peut être constitué par un système autonome ou en réseau d'archivage, de transmission et d'extraction d'images ou par un poste de visualisation comportant certaines ou la totalité des fonctions décrites ici.

Les modules de transmission évoqués plus haut, ainsi que le poste de travail 72 et les unités d'entretien 24, peuvent être reliés à la structure de services 22 par l'intermédiaire d'un réseau 80 d'accès à distance. A cette fin, n'importe qu'elle connexion en réseau peut être employée. Les configurations de réseaux préférées comprennent des réseaux exclusifs ou spécialisés ainsi que des réseaux ouverts tels que l'Internet. Des données peuvent être échangées entre les systèmes d'établissement de diagnostics, les unités d'entretien 24 et la structure centrale de services 22 sous n'importe quel format adéquat, par exemple conformément au protocole Internet (IP), au protocole de communication (TCP) ou à d'autres protocoles connus. De plus, certaines des données peuvent être transmises ou formatées en utilisant des langages de balisage tels que le langage HTML ou d'autres langages classiques. Les structures d'interface et les organes de transmission préférés sont décrits plus en détail ci-après.

Au sein de la structure de services 22, des messages, des demandes de services et des données sont reçus par des organes de transmission désignés globalement sous le repère 82. Les organes 82 transmettent les données de services à un système central de traitement de services, désigné globalement par le repère 84 sur la Fig. 1. Le système de traitement gère la réception, les manipulations et la transmission de données de services en direction et à partir de la structure de services. D'une manière générale, le système de traitement 84 peut comporter un seul ou plusieurs ordinateurs, ainsi que des serveurs matériels ou logiciels spécialisés pour traiter les différentes demandes de services et pour recevoir et émettre les données de service, comme décrit plus en détail ci-après. La structure 22 de services comporte également un ensemble de postes de travail 86 d'opérateurs, sur lesquels peuvent intervenir des techniciens d'entretien qui répondent aux demandes de services et assurent un service en différé et en direct pour les systèmes d'établissement de diagnostics en réponse aux demandes de services. Par ailleurs, le système de traitement 84 peut être en liaison avec un système de bases de données ou autres systèmes de traitement 88 dans la structure de services 22 ou à distance de ladite structure. Ces systèmes de bases de données et de traitement

peuvent contenir de grandes quantités d'informations sous forme de bases de données, concernant des paramètres de fonctionnement, des historiques d'entretien, etc., à la fois pour des scanners à abonnement particulier et pour de vastes populations d'équipements diagnostiques. Comme décrit ci-après, ces bases de données peuvent servir à la fois pour l'entretien de systèmes d'établissement de diagnostics particuliers et pour suivre cet entretien, ainsi que pour obtenir des données comparatives utilisables pour l'entretien d'un système particulier ou d'une famille de systèmes.

La Fig. 2 est un schéma de principe illustrant par une vue fonctionnelle les éléments précités du système. Comme représenté sur la Fig. 2, des unités d'entretien 24 distantes et des systèmes d'établissement de diagnostics 12 peuvent être mis en liaison avec la structure centrale de services 22 par l'intermédiaire d'une connexion en réseau désignée globalement par le repère 80. Dans chaque système d'établissement de diagnostics 12, une plate-forme uniforme 90 de services est présente. La plate-forme 90 comprend des éléments matériels, micrologiciels et logiciels permettant de formuler et de transmettre des demandes de services et des listes de tâches d'entretien, d'émettre et de recevoir des données de services, d'établir des connexions en réseau et de gérer des conditions financières ou d'abonnement entre le système d'établissement de diagnostics et la structure de services. De préférence, la plate-forme 90 est intégrée dans le dispositif de commande du système d'établissement de diagnostics. Ces plates-formes constituent une interface utilisateur graphique uniforme dans chaque système d'établissement de diagnostics, et celle-ci peut être adaptée à divers modes de fonctionnement des systèmes pour faciliter l'interaction de cliniciens et de radiologues avec les divers systèmes d'établissement de diagnostics pour des fonctions d'entretien. Les plates-formes permettent au concepteur d'un scanner de disposer d'un interfaçage direct avec les circuits de commande des différents scanners, ainsi qu'avec des dispositifs de mémoires dans les scanners, pour accéder à des fichiers d'images, des fichiers journaux et autres fichiers similaires nécessaires pour effectuer des prestations de services demandées ou faisant l'objet d'abonnements. Si un poste de gestion 70 est présent, une plate-forme uniforme similaire est de préférence chargée sur le poste de gestion pour faciliter un interfaçage direct entre le poste de gestion et la structure de services. En plus de la plate-forme uniforme 90 de services, chaque système d'établissement de diagnostics est de préférence pourvu d'un autre module de transmission 92 tel qu'un module de transmission par télécopie pour envoyer et recevoir des messages par télécopie entre le scanner distant et la structure centrale de services.

Les messages et les données transmis entre les systèmes d'établissement de diagnostics et la structure de services franchissent une barrière de sécurité ou "coupe-feu" contenue dans le système de traitement 84, ce qui empêche, d'une manière globalement connue dans la technique, d'accéder sans autorisation à la structure de services. Un châssis 96 supportant une série de modems 98 reçoit les données d'arrivée et transmet les données de départ par l'intermédiaire d'un routeur 100 qui gère la circulation des données entre les modems et le système de traitement 84 du centre de services.

Comme indiqué plus haut, le système de traitement 84 reçoit et traite les demandes de services et les données et réalise un interfaçage avec d'autres organes de service, aussi bien dans la structure de services qu'à distance de la structure. Comme représenté sur la Fig. 2, des postes de travail 86 d'opérateurs sont couplés au système de traitement, tout comme des bases de données distantes ou des ordinateurs distants 88. En outre, au moins une base 102 de données locale de services est prévue pour vérifier les droits d'utilisation et les dispositions contractuelles, pour stocker des fichiers de comptes rendus de services, des fichiers journaux, etc. De plus, un ou plusieurs modules de transmission 104 sont en liaison avec le système de traitement 84 pour envoyer et recevoir des télécopies entre la structure de services et le système d'établissement de diagnostics ou les unités d'entretien.

La Fig. 3 représente les divers organes constituant la plate-forme uniforme 90 de services dans chaque système d'établissement de diagnostics 12. Cette plate-forme uniforme de services peut être utilisée, dans la forme préférée de réalisation de l'invention, pour faciliter l'accès de systèmes distants à des applications logicielles sur un réseau. La plate-forme uniforme réside sous la forme d'un logiciel stocké dans un serveur Web 119. Le serveur Web 119 facilite l'échange de données entre le système d'établissement de diagnostics et la structure de services et permet d'examiner une série de pages Web 123 et 125 à l'aide d'un navigateur Web 121. De préférence, le serveur 119 et le navigateur 121 permettent des applications HTTP et le navigateur supporte des applications Java. La page Web principale 123 est de préférence une page en langage de balisage telle qu'une page HTML affichée pour l'utilisateur du système sur un écran présent dans le système d'établissement de diagnostics. De préférence, la page Web principale 123 est accessible depuis une page de fonctionnement normale sur laquelle l'utilisateur configurera des demandes d'examens, consultera les résultats des examens, etc., notamment à l'aide d'une icône affichée sur un écran. Par l'intermédiaire de la page Web principale 123, une série de pages Web supplémentaires 125 sont accessibles.

Ces pages Web permettent de composer des demandes de services et des demandes d'accès à des applications logicielles et de transmettre ces données à la structure centrale de services, et elles facilitent l'échange d'autres messages, comptes rendus, logiciels, protocoles, etc. comme décrit plus en détail ci-après. Le serveur Web 119 communique avec un réseau par l'intermédiaire d'un modem 131. Un module 127 de services de connectivité permet un interfaçage avec le serveur Web 119. Un module 129 de protocole point à point (PPP) est également prévu pour transmettre des paquets à protocole Internet (IP) sur des connexions de communications à distance. Comme le comprendront les spécialistes de la technique, divers autres protocoles et organes de réseaux peuvent être employés pour faciliter les échanges de données sur un réseau.

Un système de gestion de groupes peut être intégré dans le système de traitement du centre de services illustré sur la Fig. 2. Selon une autre possibilité, le système de gestion de groupes présenté ici peut être un système autonome. Les formes préférées de réalisation du système de gestion de groupes sont globalement représentées sur les figures 4 et 5. Dans chaque forme de réalisation, le système comprend une multitude de serveurs Web répartis 110 qui communiquent avec au moins un serveur décisionnel 114 à travers un coupe-feu 138. Chaque serveur Web 110 est programmé pour permettre d'accéder à une ou plusieurs applications logicielles, qui peuvent résider dans le serveur Web lui-même ou peuvent résider dans des serveurs d'applications respectifs connectés au serveur Web 110. Les serveurs Web communiquent avec des systèmes distants par l'intermédiaire de réseaux. Les applications logicielles peuvent être protégées, en ce sens que leur accès nécessite un niveau d'habilitation, ou libres au sens qu'elles sont accessibles librement à toute personne connectée au réseau. Comme expliqué plus en détail ci-après, les applications logicielles protégées dans le système préféré de gestion de groupes se répartissent en deux catégories : (1) celles qui nécessitent un niveau d'habilitation à un seul facteur (par exemple un mot de passe) pour y accéder ; et (2) celles qui nécessitent un niveau d'habilitation à deux facteurs (par exemple un mot de passe et un numéro de code de sécurité généré de manière aléatoire). La Fig. 4 sert à représenter une partie d'un système de gestion de groupes employant un niveau d'habilitation à un seul facteur, tandis que la Fig. 5 sert à représenter une partie d'un système de gestion de groupes employant un niveau d'habilitation à deux facteurs. La Fig. 5 est différente de la Fig. 4 en ce qu'elle comporte en plus un serveur de sécurité 126 qui communique avec le serveur décisionnel 114 et qui est programmé pour authentifier le deuxième facteur du test d'habilitation à deux facteurs, comme décrit plus en détail ci-après.

Les systèmes distants qui accèdent aux serveurs Web peuvent être constitués par des systèmes établissant des diagnostics médicaux, dont des systèmes d'imagerie et de contrôle. Par exemple, la Fig. 4 représente un navigateur 104 d'un scanner d'imagerie et un navigateur 106 d'un ordinateur personnel pour un service hospitalier, chacun d'eux pouvant accéder à un serveur Web 110 par l'intermédiaire d'un réseau 80 à accès distant, ainsi qu'un navigateur 108 pouvant accéder à un serveur Web 110 par l'intermédiaire de l'Internet 81. Chaque serveur Web 110 est programmé avec un module intermédiaire 112 pour intercepter des demandes d'accès, déterminer si le logiciel demandé est libre ou protégé et, s'il est protégé, pour prendre contact avec un serveur décisionnel 114. Le module intermédiaire 112 constitue une interface pour les communications entre le serveur Web 110 et le serveur décisionnel 114.

La forme de réalisation préférée comprend en outre une base de données 116 de gestion de groupes. Globalement, la base de données 116 comprend des données de sites distants, des données de contrats ou d'abonnements, des données de contacts ou d'utilisateurs et des règles commerciales (c'est-à-dire des définitions de groupes). Au sens de la présente description, le terme "groupe" désigne un groupe d'utilisateurs de systèmes distants ayant un ensemble particulier de droits d'accès. Au sens de la présente description, l'expression "application logicielle" est entendue comme couvrant un logiciel de n'importe quel type, y compris mais d'une manière nullement limitative la programmation d'applications, des fichiers de configuration, des protocoles, des fichiers de données, des listes de tâches, des comptes rendus d'interventions, des outils d'intervention, des historiques de systèmes, des données de fonctionnement de systèmes, des informations exclusives sur le logiciel utilisé dans des systèmes distants établissant des diagnostics médicaux, des techniques de réparation, des fiches commerciales et autres. Les règles commerciales stockées dans la base de données 116 de gestion de groupes fournissent les critères servant à déterminer les applications logicielles pour lesquelles un membre d'un groupe particulier possède des droits d'accès. Les données de contacts ou d'utilisateurs figurant dans la base de données 116 comprennent des noms d'utilisateurs, des mots de passe, des codes de sécurité, des numéros fictifs, des délais d'activation de génération de numéros aléatoires, la position professionnelle ou le titre d'utilisateurs et autres informations. Les données de contrats comprennent des informations sur les applications logicielles auxquelles les parties qui souscrivent un abonnement ont le droit d'accéder en vertu de contrats existants passés entre des structures distantes et la structure centrale de services. Les données de sites comprennent des informations identifiant les sites distants et les équipements utilisés sur

ces sites, dont des numéros de série des machines d'établissement de diagnostics et d'imagerie.

La forme préférée de l'invention comprend des serveurs Web 110 pour permettre un accès sélectif à des applications logicielles à haut niveau de protection, c'est-à-dire nécessitant un niveau d'habilitation à deux facteurs. Les applications logicielles ayant ce haut niveau de sécurité doivent comporter un logiciel lié aux services et utilisé par un technicien d'entretien pour réparer, remettre en état, améliorer ou entretenir un système distant d'établissement de diagnostic, par exemple des outils de services 128 et des fiches de services 130 représentés sur la Fig. 5. Par exemple, un technicien d'entretien employé par la structure centrale de services peut se voir attribuer un niveau d'habilitation à deux facteurs qui permettrait un accès distant, par exemple par l'intermédiaire du navigateur d'un scanner d'imagerie distant et par l'intermédiaire d'un réseau, à des applications logicielles nécessaires à l'entretien de ce scanner d'imagerie. Le premier facteur est le même facteur que celui utilisé pour le niveau d'habilitation à un seul facteur et il est authentifié par le serveur décisionnel 114. Selon la forme de réalisation préférée représentée sur la Fig. 5, un serveur de sécurité 126 est programmé pour authentifier le deuxième facteur du niveau d'habilitation à deux facteurs dans le cadre de la gestion du serveur décisionnel 114.

Le procédé préféré pour traiter les habilitations est illustré sur la Fig. 6. Chaque système distant est programmé avec une interface utilisateur du type représenté sur la Fig. 3 pour accéder à un serveur Web 110 par l'intermédiaire du réseau 80, par exemple un Intranet. Une des pages Web 124 peut être une page Web d'applications qui affiche une multitude de touches virtuelles de sélection d'applications pour sélectionner l'une quelconque d'une multitude d'applications logicielles accessibles à distance, liées à des services (libres ou protégés) qui résident dans les serveurs Web 110. Aux fins de la présentation, on suppose que l'accès aux applications logicielles protégées résidant dans les serveurs Web 110 représentés sur la Fig. 4 nécessite un niveau d'habilitation à un seul facteur. En revanche, l'accès à au moins une des applications logicielles protégées résidant dans un serveur Web 110 représenté sur la Fig. 5 nécessite un niveau d'habilitation à deux facteurs, ce qui implique la présence du serveur de sécurité 126. En outre, il doit être entendu que certaines applications logicielles peuvent être libres et non protégées. Cependant, l'invention concerne principalement la prise en charge de l'accès à distance à des applications logicielles protégées.

En réponse à la sélection, par l'utilisateur du système, d'une application logicielle protégée sur l'écran d'un navigateur Web, le serveur Web 119 présent dans le

système distant envoie au réseau, par l'intermédiaire des blocs 127, 129, et 131 représentés sur la figure 3, une demande d'accès à l'application logicielle sélectionnée (étape 160 de la figure 6). De préférence, l'adresse URL du serveur Web 110 où réside l'application logicielle sélectionnée comporte un code figé dans le système distant, cette adresse URL étant automatiquement jointe à la demande d'accès avant la connexion au réseau.

La demande d'accès du système distant au serveur Web consulté 110 est immédiatement interceptée par le module intermédiaire 112 de ce serveur Web, lequel module détermine tout d'abord si la demande d'accès concerne une application logicielle libre ou protégée. Si l'application logicielle est libre, c'est-à-dire disponible sans niveau d'habilitation, le module intermédiaire envoie une instruction correspondante au serveur Web et l'application est délivrée au système distant. La Fig. 6 illustre le procédé d'approbation des demandes d'accès à un logiciel protégé.

Si l'application logicielle demandée nécessite un niveau d'habilitation, le module intermédiaire détermine alors si l'utilisateur du système distant qui fait la demande a déjà été authentifié (étape 162 de la Fig. 6), c'est-à-dire s'il a déjà réalisé une ouverture de session. Si l'utilisateur a déjà eu l'occasion d'ouvrir une session, l'étape d'authentification est omise et le serveur décisionnel détermine immédiatement si l'accès demandé est autorisé (étape 168). Si l'utilisateur de système distant qui fait la demande n'a pas ouvert de session, le serveur Web sollicité télécharge vers le navigateur Web distant une fenêtre qui contient des champs pour y entrer le nom, le mot de passe et le code de sécurité de l'utilisateur. Ensuite, l'utilisateur du système distant entre les informations d'identification d'utilisateur dont a besoin le serveur décisionnel (étape 164). Dans le cas d'un utilisateur ayant un niveau d'habilitation à un seul facteur, l'utilisateur entre de préférence un nom d'utilisateur et un mot de passe ; dans le cas d'un utilisateur à niveau d'habilitation à deux facteurs, l'utilisateur entre de préférence un nom d'utilisateur, un mot de passe et un code de sécurité généré par un générateur de numéros aléatoires, générateur que possède l'utilisateur. Le serveur Web 119 du système distant (cf. Fig. 3) envoie alors sur le réseau les informations entrées concernant l'utilisateur, adressées au serveur Web 110 (cf. figures 4 et 5) où réside l'application logicielle demandée. Les informations transmises concernant l'utilisateur sont interceptées par le module intermédiaire 112 et transmises au serveur décisionnel 114 ainsi qu'un code identifiant l'application logicielle protégée concernée par la demande d'accès.

Dans le cas de niveaux d'habilitation à un seul facteur, le serveur décisionnel authentifie le mot de passe (étape 166) en consultant la base de données 124 d'utilisateurs, qui fait partie de la base de données de gestion de groupes. Dans la forme de réalisation la plus simple, la base de données d'utilisateurs stocke un mot de passe correspondant à chaque nom d'utilisateur et le serveur décisionnel a seulement à extraire ce mot de passe et à le comparer avec le mot de passe reçu du module intermédiaire où réside le logiciel demandé. Si le mot de passe n'est pas authentique, le serveur Web consulté envoie un message d'erreur au système distant. Si le code d'utilisateur est authentique, le serveur décisionnel doit déterminer ensuite si l'accès demandé est autorisé (étape 168). Dans le cas de niveaux d'habilitation à deux facteurs, le serveur décisionnel authentifie un mot de passe tout en déléguant au serveur de sécurité l'authentification d'un code de sécurité correspondant (étape 165). Si le mot de passe et le code de sécurité sont authentiques, le serveur décisionnel passe à la phase d'autorisation (étape 168).

Selon la forme préférée de réalisation de l'invention, le serveur décisionnel est programmé pour déterminer si l'utilisateur du système distant est autorisé à accéder à l'application logicielle protégée, en exécutant les étapes suivantes, consistant à : extraire de la base de données de gestion de groupes des critères d'autorisation (c'est-à-dire des règles commerciales ou des définitions de groupes 118) pour l'application logicielle protégée ; extraire de la base de données de gestion de groupes des informations pour une ou plusieurs variables (à savoir des informations sur l'utilisateur, le site, le système et le contrat) ; et déterminer si ces variables répondent à ces critères d'autorisation. Le serveur décisionnel 114 extrait de la base de données de gestion de groupes la totalité des données utiles pour l'utilisateur identifié d'un système distant et stocke ces données extraites dans une mémoire cache interne d'ouverture de session. D'après les critères et les données de variables extraits pendant l'étape d'autorisation 168, le serveur décisionnel 114 détermine si l'utilisateur de système distant qui effectue une demande a des droits d'accès à l'application logicielle demandée (étape 170).

Si l'utilisateur de système distant qui effectue la demande est autorisé à accéder à l'application logicielle protégée demandée, le serveur décisionnel délivre alors une instruction au module intermédiaire où réside le logiciel protégé afin de permettre l'accès. Ensuite, le serveur Web correspondant télécharge l'application logicielle protégée dans le système distant où l'utilisateur qui fait une demande (étape 178) a ouvert une session. Par suite du téléchargement, le serveur Web (cf. Fig. 3) présent dans

le système distant affiche sur le navigateur 121 la page Web d'ouverture de l'application logicielle téléchargée.

Eventuellement, l'algorithme représenté sur la Fig. 6 comprend l'étape 174 consistant à déterminer si l'application logicielle doit être personnalisée avant d'être fournie, par exemple en comportant un message d'accueil dans lequel on s'adresse à l'utilisateur par son nom. Les services éventuels de personnalisation sont assumés par le serveur Web 110 (cf. Fig. 4) lors de l'étape 176. L'application personnalisée est ensuite transmise au site distant lors de l'étape 178.

Le serveur décisionnel est en outre programmé pour demander au module intermédiaire du serveur Web où réside le logiciel demandé de refuser l'accès si l'utilisateur du système distant est un membre d'un groupe non autorisé à accéder à ce logiciel protégé. Eventuellement, le serveur Web où réside le logiciel protégé est programmé pour transmettre au système distant une liste indiquant toutes les applications logicielles pour lesquelles l'utilisateur de système distant qui fait une demande a des droits d'accès (étape 172), en réponse à un refus d'accès par le serveur décisionnel.

Selon une forme de réalisation préférée, l'étape 162 (cf. Fig. 6) consistant à déterminer que le code de l'utilisateur a déjà été authentifié, c'est-à-dire que l'utilisateur du système distant a déjà réussi à ouvrir une session, est exécutée de la manière suivante. Le navigateur Web présent dans chaque système distant et le module intermédiaire dans chaque serveur Web d'applications comportent une mémoire cache d'ouverture de session pour stocker les paramètres entrés par l'utilisateur (par exemple, le nom, le mot de passe et le code de sécurité de l'utilisateur) et une étiquette d'authenticité correspondante qui est générée après authentification par le serveur décisionnel. Voici la suite d'opérations. (1) L'utilisateur du système distant transmet une demande d'accès à un premier serveur Web. (2) Le premier serveur Web télécharge alors une page Web demandant à l'utilisateur du système distant d'ouvrir la session. (3) L'utilisateur du système distant entre alors un nom et un mot de passe d'utilisateur (niveau d'habilitation à un seul facteur), ou un nom, un mot de passe et un code de sécurité d'utilisateur (niveau d'habilitation à deux facteurs) à l'aide de l'interface utilisateur et envoie ces données entrées au premier serveur Web, les informations concernant l'utilisateur étant automatiquement stockées dans la mémoire cache d'ouverture de session d'un navigateur Web. L'opérateur du premier serveur Web intercepte les informations entrées concernant l'utilisateur et les envoie au serveur décisionnel. (5) Si les informations concernant l'utilisateur sont authentiques, le serveur

décisionnel adjoint une étiquette d'authenticité, stocke les informations concernant l'utilisateur et l'étiquette d'authenticité dans sa mémoire cache d'ouverture de session et renvoie ces données à l'opérateur du premier serveur Web. (6) Les mêmes données sont ensuite stockées dans la mémoire cache d'ouverture de session du module intermédiaire et sont renvoyées au système distant, les informations concernant l'utilisateur et l'étiquette d'authenticité étant stockées dans la mémoire cache d'ouverture de session du navigateur Web. (7) Lorsque l'utilisateur du système distant transmet ensuite à un deuxième serveur Web une demande d'accès, les informations concernant l'utilisateur et l'étiquette d'authenticité stockées dans la mémoire cache d'ouverture de session du navigateur Web sont envoyées automatiquement à ce deuxième serveur Web. (8) L'opérateur du deuxième serveur Web relaie alors en direction du serveur décisionnel les informations relatives à l'utilisateur et l'étiquette d'authenticité reçue. (9) Si les informations concernant l'utilisateur et l'étiquette d'authenticité envoyées par le deuxième serveur Web correspondent aux informations concernant l'utilisateur et l'étiquette d'authenticité stockées dans la mémoire cache d'ouverture de session du serveur décisionnel, le serveur décisionnel envoie alors au deuxième serveur Web un signal indiquant que le code d'utilisateur est authentique. Ainsi, le deuxième serveur Web sait qu'il peut sauter l'étape de téléchargement de la page Web d'ouverture de session vers le système distant. Ces opérations rendent inutile, pour un utilisateur de système distant demandant de multiples applications logicielles, l'ouverture de multiples sessions. Au contraire, une seule ouverture de session suffit, quel que soit le nombre de demandes d'accès à des applications logicielles faites par un utilisateur distant qui a ouvert une session.

Selon un autre aspect de la présente invention, l'accès à des applications logicielles à haut niveau de protection nécessite un niveau d'habilitation à deux facteurs. Comme décrit plus haut, le premier facteur est un mot de passe secret associé à un nom d'utilisateur. Le deuxième facteur est un numéro généré de façon aléatoire que l'utilisateur d'un système distant extrait d'un dispositif portable, tel qu'un dispositif de poche, qu'il porte. Le dispositif portable contient un générateur de numéros aléatoires servant à générer en continu des numéros conformément à un algorithme en mémoire de génération de numéros aléatoires, ainsi qu'un écran d'affichage qui affiche la valeur instantanée dans l'ordre de numéros générés de façon aléatoire. Le générateur de numéros aléatoires est activé par la structure centrale de services en commençant par un numéro fictif entré dans le dispositif portable par le prestataire central de services. Le moment de l'activation de la génération de numéros aléatoires est ensuite stocké dans la

base de données d'utilisateurs, ainsi que le nom, le mot de passe, le numéro fictif de l'utilisateur et d'autres informations concernant l'utilisateur.

En fonction de la présence d'un code de sécurité dans les informations concernant l'utilisateur reçues de l'utilisateur du système distant via le module intermédiaire 112 (cf. Fig. 5), le serveur décisionnel 114 constate qu'un niveau d'habilitation à deux facteurs est présent pour délivrer une autorisation. Sur la base du nom d'utilisateur, le serveur décisionnel 114 extrait alors les informations concernant cet utilisateur de la base de données 116 de gestion de groupes. Le serveur décisionnel 114 compare le mot de passe entré avec le mot de passe extrait de la base de données. S'ils coïncident, le serveur décisionnel envoie alors au serveur de sécurité 126 le code de sécurité entré par l'utilisateur et le numéro fictif et le moment d'activation pour la génération de numéros aléatoires, extraits de la base de données. D'après le moment d'activation et le numéro fictif reçus du serveur décisionnel et l'algorithme de génération de numéros aléatoires stocké dans le serveur de sécurité (qui est le même algorithme que celui contenu dans le générateur de numéros aléatoires porté par l'utilisateur), le serveur de sécurité génère un numéro aléatoire destiné à servir de code de sécurité de référence. Le code de sécurité entré par l'utilisateur est authentifié s'il se situe dans des limites prédéterminées du code de sécurité de référence. Le serveur de sécurité informe ensuite le serveur décisionnel des résultats de la comparaison. Si le code de sécurité entré est authentique, le serveur décisionnel passe alors à l'étape d'autorisation. Si le code de sécurité n'est pas authentique, le serveur décisionnel demande au module intermédiaire concerné de refuser l'accès à l'application logicielle demandée. Le module intermédiaire peut alors demander à l'utilisateur du système distant de tenter une nouvelle ouverture de session.

La Fig. 7 illustre des exemples d'organes pour une structure de services 22 mettant en œuvre la présente invention. Comme indiqué plus haut, la structure de service 22 comprend un châssis 96 de modems comportant une pluralité de modems 98 couplés à un routeur 100 pour coordonner la transmission de données avec la structure de services. Un serveur 94 de services HTTP appelé "réception" reçoit et oriente les transactions d'arrivée et de départ avec la structure. De préférence, les serveurs Web d'applications sont également disposés en face du coupe-feu 138. Un seul serveur Web 110 d'applications comportant un module intermédiaire 112 est représenté sur la Fig. 6. Les serveurs 94 et 110 sont couplés aux autres organes de la structure par l'intermédiaire d'un coupe-feu 138 pour la sécurité du système. Des postes de travail 86 d'opérateurs sont couplés au gestionnaire de ports pour traiter les demandes de services et

transmettre des messages et des comptes rendus en réponse à ces demandes. Une unité de services automatisée 136 peut également faire partie de la structure de services pour répondre automatiquement à certaines demandes de services, en parcourant des systèmes d'établissement de diagnostics à abonnement pour trouver des données de paramètres de fonctionnement, etc. Dans une forme de réalisation préférée, l'unité de services automatisée 136 peut fonctionner indépendamment de ou en coopération avec les organes de services interactifs constituant le système de traitement 84. Il faut souligner que d'autres types de réseaux ou de transmissions peuvent être prévus pour permettre à la structure de services de communiquer et d'échanger des données et des messages avec des systèmes d'établissement de diagnostics et des structures centrales de services, par exemple des systèmes comportant des prestataires de services extérieurs sur Internet et des réseaux privés virtuels.

Derrière le coupe-feu 138, un serveur "administratif" d'applications HTTP 140 coordonne le traitement des demandes de services, la messagerie, l'émission de comptes rendus, les transferts de logiciels, etc. D'autres serveurs peuvent être couplés au serveur d'applications HTTP 140, par exemple des serveurs 142 d'analyse de services configurés pour répondre à des types spécifiques de demandes de services. Dans la forme de réalisation représentée sur la Fig. 7, le système de traitement 84 comprend également un serveur décisionnel 114, un serveur de sécurité 126 et un serveur de licence 144. Le serveur décisionnel et le serveur de licence sont tous deux couplés à une base de données 146 de décisions/licences, qui doit comporter la base de données de gestion de groupes évoquée plus haut, ainsi qu'une base de données de licences. Le module de licence 144 assure les fonctions de stockage, de mise à jour et de vérification de l'état des abonnés et des contrats régissant l'entretien des systèmes d'établissement de diagnostics. Selon une autre possibilité, le serveur 144 de licences peut être disposé à l'extérieur du coupe-feu 138 pour vérifier l'état des abonnements avant une admission dans la structure de services. Le serveur décisionnel 114 assure les fonctions précédemment décrites ici en référence aux figures 4 à 6. Le serveur 144 de licences génère des licences, installe sur les systèmes distants 12 les licences générées à l'aide du réseau 80 et enregistre les licences dans la base de données 146 de décisions/licences. Par l'intermédiaire du réseau, le serveur 144 de licences a également la possibilité de supprimer ou de résilier une licence existante depuis un système distant.

La gestion des demandes de services, des échanges de messages et de l'émission de comptes rendus est coordonnée par un module de planification couplé au serveur HTTP 140. Le module de planification 148 coordonne les activités d'autres

serveurs constituant le système de traitement, par exemple un serveur 150 de comptes rendus, un serveur 152 de messages et un serveur 154 de téléchargement de logiciels. Comme le comprendront les spécialistes de la technique, les serveurs 150, 152 et 154 sont couplés à des dispositifs de mémoires (non représentés) servant à stocker des données telles que des listes de tâches, des adresses, des fichiers journaux, des fichiers de messages et de comptes rendus, un logiciel d'applications, etc. En particulier, comme illustré sur la Fig. 7, le serveur 154 de logiciels est couplé par l'intermédiaire d'un ou de plusieurs canaux de transmission de données à un dispositif de stockage 156 servant à contenir des progiciels transmissibles qui peuvent être directement envoyés aux systèmes d'établissement de diagnostics, auxquels les systèmes d'établissement de diagnostics peuvent accéder, ou fournis sur la base d'une facturation à la prestation ou d'un achat. Les serveurs 152 et 154 de messages et de comptes rendus sont en outre couplés, ainsi que le module de transmission 104, à un module 158 de gestion de délivrance, qui est configuré pour recevoir des messages de départ, assurer une bonne connectivité avec les systèmes d'établissement de diagnostics et coordonner la transmission de messages aux systèmes d'établissement de diagnostics et la transmission de messages et de listes de tâches à des techniciens d'entretien situés à distance, par l'intermédiaire du réseau.

Dans une forme de réalisation préférée, les circuits fonctionnels précités peuvent-être configurés sous la forme de matériels, de progiciels ou de logiciels sur n'importe quelle plate-forme informatique appropriée. Par exemple, les circuits fonctionnels des systèmes d'établissement de diagnostics peuvent être programmés sous la forme d'un code approprié dans un ordinateur personnel ou sur un poste de travail, soit entièrement intégré dans le scanner du système, soit ajouté dans le scanner. Les circuits fonctionnels de la structure de services peuvent comporter des ordinateurs personnels ou des postes de travail supplémentaires, en plus d'un ordinateur central dans lequel sont configurés un ou plusieurs des serveurs, le module de planification, etc. Enfin, les unités d'entretien peuvent comporter des ordinateurs personnels ou des ordinateurs portables de n'importe quelle plate-forme de traitement appropriée. Il faut également souligner que les circuits fonctionnels précités peuvent être adaptés de toutes sortes de manières pour exécuter les fonctions décrites ici. D'une manière générale, les circuits fonctionnels facilitent l'échange de données de services entre les systèmes d'établissement de diagnostics et une structure centrale de services, les échanges étant de préférence réalisés d'une manière interactive pour effectuer des actualisations régulières pour les systèmes d'établissement de diagnostics des activités de services.

Bien que la forme de réalisation préférée décrite emploie des modems pour faciliter les communications avec un réseau d'accès à distance, il doit être entendu que des modems ne sont pas indispensables pour mettre en œuvre l'invention. En particulier, on peut utiliser l'Internet ou des réseaux privés.

L'expression "application logicielle" utilisée dans les revendications est destinée à couvrir un logiciel de n'importe quel type, comprenant d'une façon nullement limitée la programmation d'applications, des fichiers de configuration, des protocoles, des fichiers de données, des listes de tâches, des comptes rendus d'entretien, des historiques de systèmes, des outils de services, des données de fonctionnement de systèmes, des documents exclusifs, des techniques de réparation, des fiches commerciales, et autres.

REVENDICATIONS

1. Procédé pour autoriser l'accès à une application logicielle protégée par un utilisateur d'un système distant d'établissement de diagnostics médicaux à l'aide d'un réseau, ladite application logicielle protégée étant stockée dans une structure centrale et nécessitant un niveau d'habilitation pour être accessible, le procédé comprenant les étapes consistant en ce que :

ledit utilisateur de système distant envoie une demande d'accès (160) à ladite structure centrale par l'intermédiaire dudit réseau ;

ledit utilisateur de système distant envoie une identification d'utilisateur et un mot de passe (164) à ladite structure centrale par l'intermédiaire dudit réseau ;

ladite structure centrale détermine si ledit mot de passe est authentique (166) ;

ladite structure centrale détermine si ledit utilisateur de système distant est autorisé (168) à accéder à ladite application logicielle protégée ; et par l'étape consistant à

autoriser ledit utilisateur de système distant à accéder (178) à ladite application logicielle protégée si ledit mot de passe est authentique et si ledit utilisateur de système distant est autorisé à accéder à ladite application logicielle protégée.

2. Procédé selon la revendication 1, dans lequel ladite structure centrale authentifie ledit mot de passe envoyé par ledit utilisateur de système distant en faisant concorder ledit mot de passe avec un mot de passe extrait d'une base de données de gestion de groupes.

3. Procédé selon la revendication 1, dans lequel ladite base de données de gestion de groupes stocke des mots de passe pour chaque personne autorisée à accéder à des applications logicielles à partir dudit système distant d'établissement de diagnostics médicaux par l'intermédiaire dudit réseau.

4. Procédé selon la revendication 1, dans lequel ledit utilisateur de système distant envoie ladite demande d'accès et lesdites données d'identification d'utilisateur par interaction avec un navigateur Web situé dans ledit système distant d'établissement de diagnostics médicaux .

5. Système comprenant :

un réseau (80) ;

un serveur Web (110) connecté audit réseau et comprenant un module intermédiaire (112) programmé pour permettre l'accès à une application logicielle protégée en réponse à une autorisation ;

un système distant (12) d'établissement de diagnostics médicaux ayant un navigateur Web (104) pour envoyer audit serveur Web, par l'intermédiaire dudit réseau, une demande d'accès à ladite application logicielle protégée, une identification d'utilisateur et un mot de passe ;

une base de données (116) de gestion de groupes comprenant des informations qui correspondent à des utilisateurs respectifs, des informations sur des sites, des informations sur des systèmes et des informations sur des contrats correspondant à des systèmes distants respectifs d'établissement de diagnostics médicaux, et des règles comprenant des critères d'autorisation pour déterminer l'accès à des applications logicielles protégées ; et

un serveur décisionnel (114) qui communique avec ladite base de données de gestion de groupes et avec ledit module intermédiaire, ledit serveur décisionnel étant programmé pour authentifier ledit mot de passe d'utilisateur et envoyer ladite autorisation audit module intermédiaire si ledit mot de passe est authentique et si tous les critères d'autorisation pour ladite application logicielle protégée ont été satisfaits.

6. Système selon la revendication 5, dans lequel ledit serveur décisionnel est programmé pour exécuter les étapes suivantes, consistant à :

recevoir dudit module intermédiaire ladite demande d'accès, ladite identification d'utilisateur et ledit mot de passe ;

extraire de ladite base de données de gestion de groupes un mot de passe avec ladite identification d'utilisateur reçue ; et

déterminer si ledit mot de passe extrait coïncide avec ledit mot de passe reçu.

7. Système selon la revendication 6, dans lequel ledit serveur décisionnel est programmé pour déterminer si ladite identification d'utilisateur identifie une personne autorisée à accéder à ladite application logicielle protégée en effectuant les étapes suivantes, consistant à :

extraire de ladite base de données de gestion de groupes lesdits critères d'autorisation pour ladite application logicielle protégée ;

extraire de ladite base de données de gestion de groupes des informations pour une ou plusieurs variables ; et

déterminer si lesdites variables satisfont lesdits critères d'autorisation.

8. Système selon la revendication 5, comprenant en outre un coupe-feu (138) entre ledit serveur Web et ledit serveur décisionnel.

9. Système pour autoriser l'accès à une application logicielle protégée par l'intermédiaire d'un réseau 80 pour un utilisateur d'un système distant d'établissement de diagnostics médicaux, ladite application logicielle protégée étant stockée dans une structure centrale 22 et nécessitant une autorisation d'accès, ledit système distant comprenant un moyen (104) pour envoyer une demande d'accès à ladite application logicielle protégée, une identification d'utilisateur et un mot de passe à ladite structure centrale par l'intermédiaire dudit réseau ; et ladite structure centrale comprenant des moyens (114, 116) pour déterminer si ledit mot de passe est authentique, des moyens (114, 116) pour déterminer si ledit utilisateur de système distant est autorisé à accéder à ladite application logicielle protégée, et des moyens (110, 112, 114) pour permettre audit utilisateur de système distant d'accéder à ladite application logicielle si ledit mot de passe est authentique et si ledit utilisateur de système distant est autorisé à accéder à ladite application logicielle protégée.

10. Système selon la revendication 9, dans lequel ladite structure centrale comprend en outre un moyen pour authentifier ledit mot de passe envoyé par ledit utilisateur de système distant en faisant coïncider ledit mot de passe avec un mot de passe extrait d'une base de données.

11. Système selon la revendication 9, dans lequel lesdits moyens d'autorisation d'accès comprennent un serveur Web (110) programmé pour autoriser d'une manière sélective l'accès à ladite application logicielle protégée en réponse à l'autorisation, l'accès audit serveur Web se faisant, pour ledit système distant d'établissement de diagnostics médicaux, par l'intermédiaire dudit réseau.

12. Procédé pour fournir des applications logicielles à une multitude de systèmes distants par l'intermédiaire de réseaux, comprenant les étapes consistant à :

construire une base de données de gestion de groupes, accessible de manière électronique, comprenant des informations suffisantes pour qu'un processeur puisse déterminer si un utilisateur particulier d'un système identifié par un code d'utilisateur dans ladite base de données appartient à un groupe ayant des droits d'accès à une application logicielle particulière identifiée par un code d'application dans ladite base de données ;

détecter le code d'application d'une première application logicielle demandée par un utilisateur particulier d'un système distant ;

recevoir le code d'utilisateur dudit utilisateur particulier d'un système distant par l'intermédiaire d'un réseau ;

vérifier dans ladite base de données de gestion de groupes pour déterminer si ledit utilisateur particulier de système distant est un membre d'un groupe ayant des droits d'accès à ladite première application logicielle ; et

refuser audit utilisateur particulier de système distant d'accéder à ladite première application logicielle si ledit utilisateur particulier de système distant n'est pas membre d'un groupe ayant des droits d'accès à ladite première application logicielle.

13. Procédé selon la revendication 12, comprenant en outre les étapes consistant à :

vérifier dans ladite base de données de gestion de groupes pour déterminer si ledit code d'utilisateur est authentique ; et

accorder audit utilisateur particulier de système distant l'accès à ladite première application logicielle si ledit code d'utilisateur est authentique et si ledit utilisateur particulier de système distant est membre d'un groupe ayant des droits d'accès à ladite première application logicielle.

14. Procédé selon la revendication 13, comprenant en outre les étapes consistant à :

stocker dans ledit système distant une première adresse de réseau à laquelle il est possible d'accéder à ladite première application logicielle ;

demander l'accès à ladite première application logicielle par coopération avec un navigateur Web dans ledit système distant ; et

adresser ladite demande d'accès à ladite première adresse de réseau.

15. Procédé selon la revendication 14, comprenant en ouvre les étapes consistant à :

envoyer une demande d'ouverture de session audit navigateur Web en réponse à la réception de ladite demande d'accès à ladite première adresse de réseau ;

ouvrir une session en entrant ledit code d'utilisateur par l'intermédiaire dudit navigateur Web ;

stocker ledit code d'utilisateur dans une mémoire cache d'ouverture de session présente dans ledit navigateur Web ; et

envoyer ledit code d'utilisateur à ladite première adresse de réseau en réponse à ladite ouverture de session.

16. Procédé selon la revendication 15, comprenant en outre les étapes consistant à :

stocker dans ledit système distant une deuxième adresse de réseau à laquelle il est possible d'accéder à une deuxième application logicielle ;

vérifier dans ladite base de données de gestion de groupes pour déterminer si ledit code d'utilisateur est authentique ;

si ledit code d'utilisateur est authentique, fournir une étiquette d'authenticité audit système distant pour la stocker dans ladite mémoire cache d'ouverture de session présente dans ledit navigateur Web ;

demander l'accès à ladite deuxième application logicielle par coopération avec ledit navigateur Web ; et

envoyer automatiquement ledit code d'utilisateur et ladite étiquette d'authenticité à ladite deuxième adresse de réseau ainsi que ladite demande d'accès à ladite deuxième application logicielle.

17. Procédé selon la revendication 14, comprenant en outre l'étape consistant à envoyer une liste d'applications logicielles audit navigateur Web si ledit utilisateur particulier de système distant n'est pas membre d'un groupe ayant des droits d'accès à ladite première application logicielle, ladite liste indiquant toutes les applications logicielles pour lesquelles ledit utilisateur particulier d'un système distant a des droits d'accès.

18. Procédé selon la revendication 14, comprenant en outre les étapes consistant à :

personnaliser ladite première application logicielle si ledit utilisateur particulier de système distant se voit accorder un accès ; et

délivrer ladite première application logicielle personnalisée audit navigateur Web.

19. Système comprenant :

une base de données (116) de gestion de groupes comprenant un ensemble de règles commerciales pour définir des groupes d'utilisateurs de systèmes distants, un ensemble de codes d'utilisateurs servant à identifier des utilisateurs de systèmes distants, et un ensemble de codes d'applications servant à identifier des applications logicielles pour lesquelles divers groupes d'utilisateurs de systèmes distants ont des droits d'accès ; et

un serveur décisionnel (114) programmé pour exécuter les étapes suivantes, consistant à :

recevoir un code d'utilisateur correspondant à un utilisateur de système distant qui fait une demande ;

détecter un code d'application d'une première application logicielle demandée par ledit utilisateur de système distant qui fait une demande ;

accéder à ladite base de données de gestion de groupes pour déterminer si ledit utilisateur de système distant qui fait une demande appartient à un groupe ayant des droits d'accès à ladite première application logicielle demandée ; et

délivrer un signal représentant les résultats de ladite détermination.

20. Système selon la revendication 19, comprenant en outre :

un réseau (80) ;

un premier serveur Web (110) accessible par l'intermédiaire dudit réseau et programmé pour donner d'une manière sélective accès à ladite première application logicielle ; et

un système distant (12) comprenant un moyen (130) pour accéder audit premier serveur Web par l'intermédiaire dudit réseau, un moyen (104) pour demander l'accès à ladite première application logicielle et un moyen (104) pour enregistrer ledit code d'utilisateur correspondant audit utilisateur de système distant qui fait une demande,

ledit serveur décisionnel étant programmé pour délivrer un signal représentant une instruction transmise audit premier serveur Web pour accorder l'accès à ladite première application logicielle si ledit code d'utilisateur est authentique et si ledit utilisateur de système distant a des droits d'accès à ladite première application logicielle demandée, et ledit premier serveur Web est programmé pour fournir ladite première application logicielle demandée audit système distant en réponse à ladite instruction demandant d'accorder l'accès.

21. Système selon la revendication 20, dans lequel ledit serveur décisionnel est programmé pour délivrer un signal représentant une instruction transmise audit premier serveur Web pour refuser l'accès à ladite première application logicielle si ledit utilisateur de système distant n'a pas de droit d'accès à ladite première application logicielle demandée, et ledit premier serveur Web est programmé pour fournir une liste d'applications autorisées audit système distant en réponse à ladite instruction demandant un refus d'accès.

22. Système selon la revendication 20, dans lequel ledit premier serveur Web est programmé avec un module intermédiaire (112) pour gérer les communications avec ledit serveur décisionnel.

23. Système selon la revendication 22, dans lequel ledit moyen de demande et ledit moyen d'enregistrement dudit système distant font partie d'un navigateur Web, et dans lequel ledit navigateur Web, ledit module intermédiaire et ledit serveur Web du serveur décisionnel comportent chacun une mémoire cache respective d'ouverture de session, et ledit serveur décisionnel est programmé pour générer une étiquette d'authenticité en réponse à l'authentification dudit code d'utilisateur, ladite étiquette d'authenticité étant stockée dans chacune desdites mémoires caches d'ouverture de session avec ledit code d'utilisateur.

24. Système selon la revendication 23, comprenant en outre un deuxième serveur Web (110) accessible par l'intermédiaire dudit réseau, programmé pour permettre un accès sélectif à une deuxième application logicielle, et comportant une mémoire cache d'ouverture de session, dans lequel ledit système distant comporte un moyen servant à envoyer automatiquement ledit code d'utilisateur et ladite étiquette d'authenticité audit deuxième serveur Web avec ladite demande d'accès à ladite

deuxième application logicielle, ledit deuxième serveur Web étant en outre programmé pour envoyer ledit code d'utilisateur et ladite étiquette d'authenticité audit serveur décisionnel, et ledit serveur décisionnel étant en outre programmé pour vérifier ledit code d'utilisateur et ladite étiquette d'authenticité reçus dudit deuxième serveur Web.

25. Système selon la revendication 20, dans lequel ledit moyen servant à accéder audit premier serveur Web par l'intermédiaire dudit réseau comporte une adresse de réseau à code figé dans ledit système distant.

26. Système selon la revendication 20, comportant en outre un coupe-feu (138) entre ledit premier serveur Web et ledit serveur décisionnel.

27. Système selon la revendication 20, dans lequel ledit premier serveur Web est programmé pour exécuter les étapes consistant à :

personnaliser ladite première application logicielle si l'utilisateur de système distant qui fait une demande se voit accorder l'accès ; et

fournir ladite première application logicielle personnalisée auxdits systèmes distants.

28. Système comprenant :

un réseau (80) ;

un serveur Web (110) accessible par l'intermédiaire dudit réseau et programmé pour assurer un accès sélectif à une application logicielle ;

un système distant (12) comportant un navigateur Web (104) pour demander l'accès à ladite application logicielle et enregistrer un code d'utilisateur correspondant à un utilisateur de système distant ;

une base de données (116) de gestion de groupes comportant un ensemble de règles commerciales servant à définir des groupes d'utilisateurs de systèmes distants, un ensemble de codes d'utilisateurs servant à identifier des utilisateurs de systèmes distants, et un ensemble de codes d'applications servant à identifier des applications logicielles pour lesquelles divers groupes d'utilisateurs de systèmes distants ont des droits d'accès ; et

un ordinateur (114) programmé pour gérer l'accès à ladite application logicielle par ledit utilisateur de système distant sur la base desdites règles

commerciales, desdits codes d'utilisateurs et desdits codes d'applications stockés dans ladite base de données de gestion de groupes.

29. Système selon la revendication 28, dans lequel ledit ordinateur est programmé pour délivrer audit serveur Web un signal représentant une instruction visant à accorder l'accès à ladite application logicielle si ledit utilisateur de système distant est membre d'un groupe ayant des droits d'accès à ladite application logicielle.

30. Système selon la revendication 28, dans lequel l'ordinateur est programmé pour délivrer audit serveur Web un signal représentant une instruction visant à refuser l'accès à ladite application logicielle si ledit utilisateur de système distant n'est pas membre d'un groupe ayant des droits d'accès à ladite application logicielle.

31. Système selon la revendication 28, comprenant en outre un coupe-feu (38) entre ledit premier serveur Web et ledit ordinateur.

32. Système pour fournir des applications logicielles à une multitude de systèmes distants (12) par l'intermédiaire d'un réseau (80), comprenant :

une base de données (116) de gestion de groupes, accessible de manière électronique et contenant des informations qui représentent les droits d'accès à des applications logicielles pour différents groupes d'utilisateurs de systèmes distants ; et

un ordinateur (114) programmé pour refuser à un utilisateur de système distant l'accès à une application logicielle si des données présentes dans ladite base de données de gestion de groupes indiquent que ledit utilisateur de système distant n'est pas membre d'un groupe ayant des droits d'accès à ladite application logicielle.

33. Système selon la revendication 32, dans lequel ledit ordinateur est en outre programmé pour accorder audit utilisateur de système distant l'accès à ladite application logicielle si ledit utilisateur de système distant entre un code d'utilisateur authentique et si des données présentes dans ladite base de gestion de groupes indiquent que ledit utilisateur de système distant est membre d'un groupe ayant des droits d'accès à ladite application logicielle.

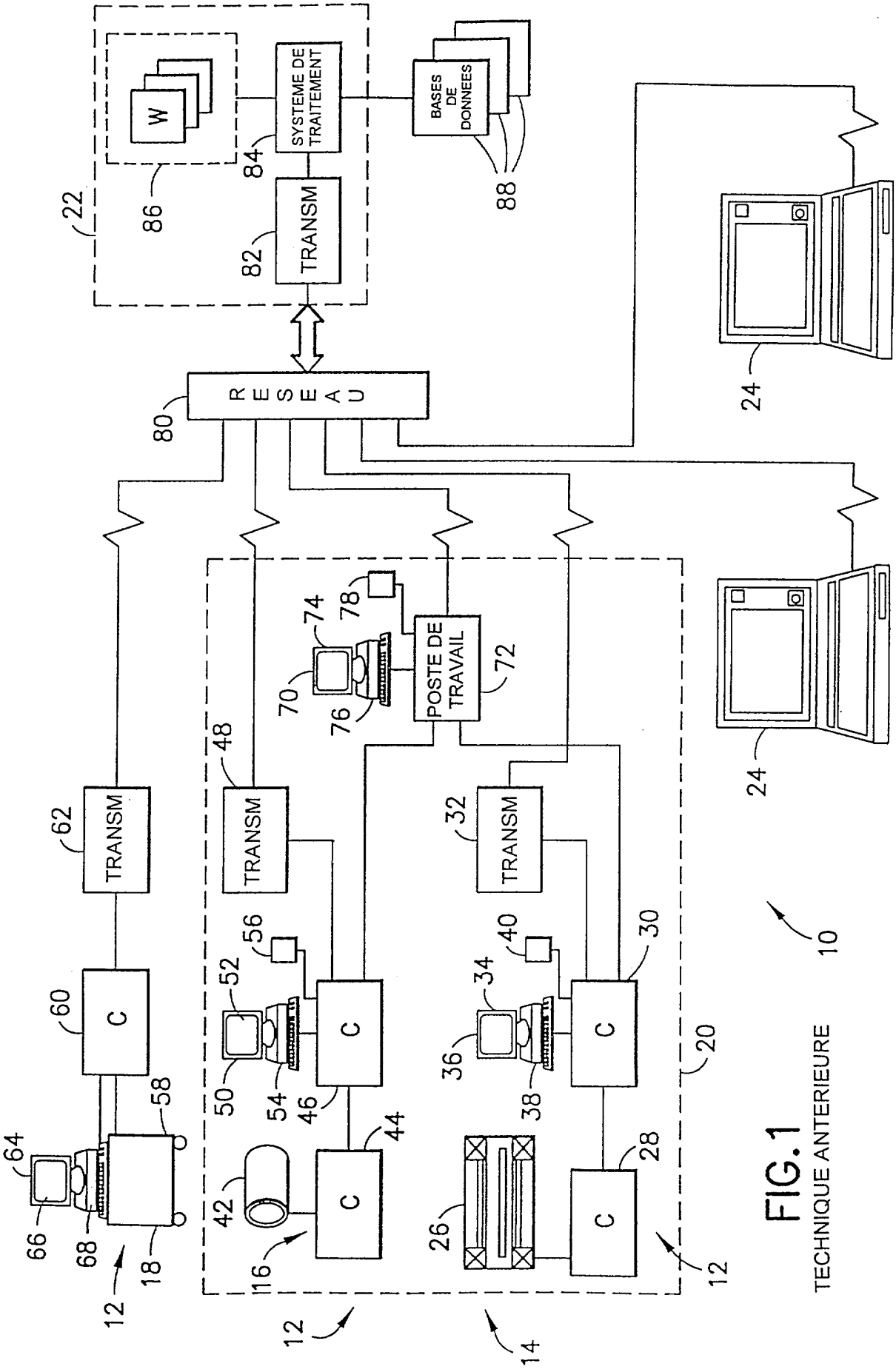


FIG.1

TECHNIQUE ANTERIEURE

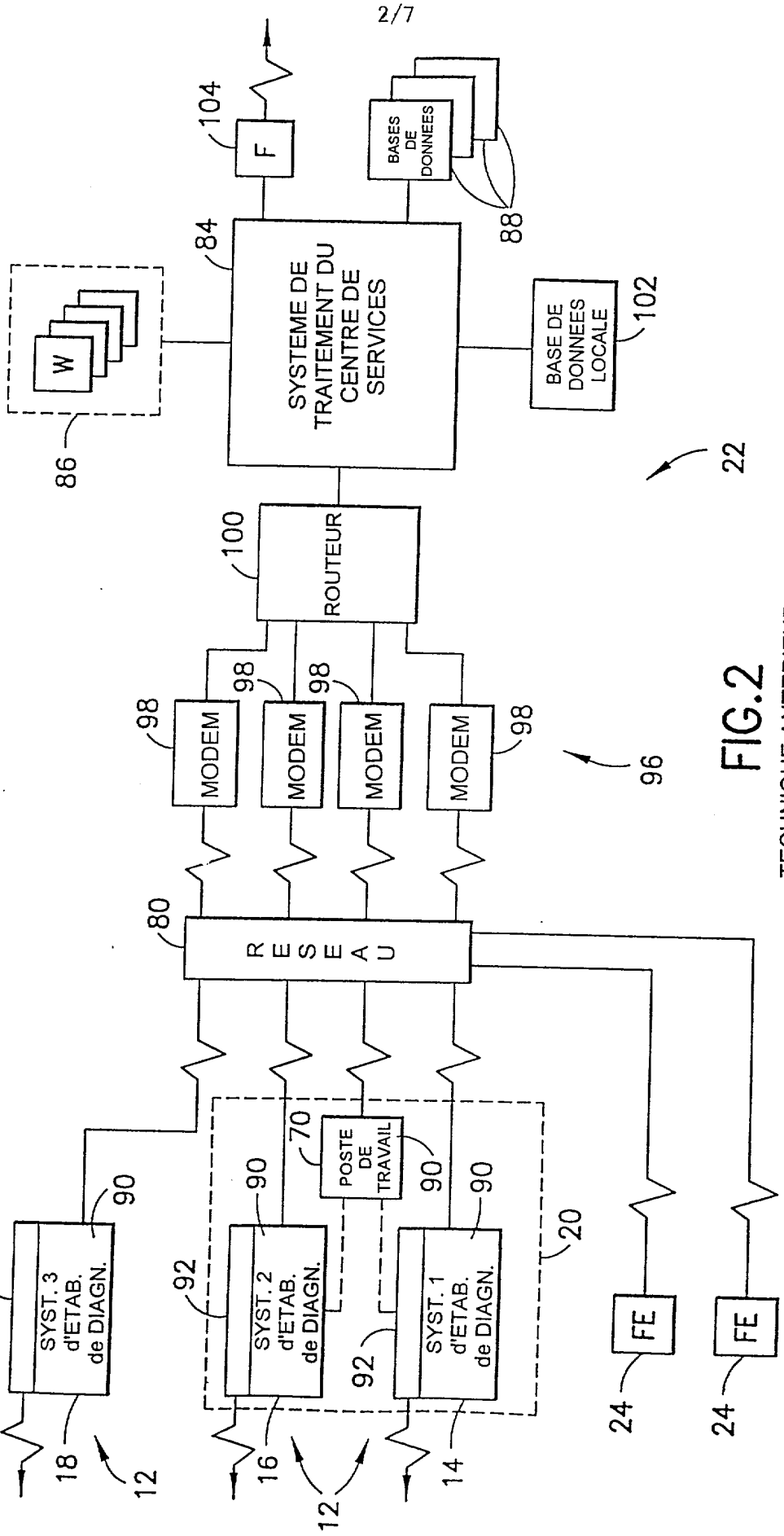


FIG.2

TECHNIQUE ANTERIEURE

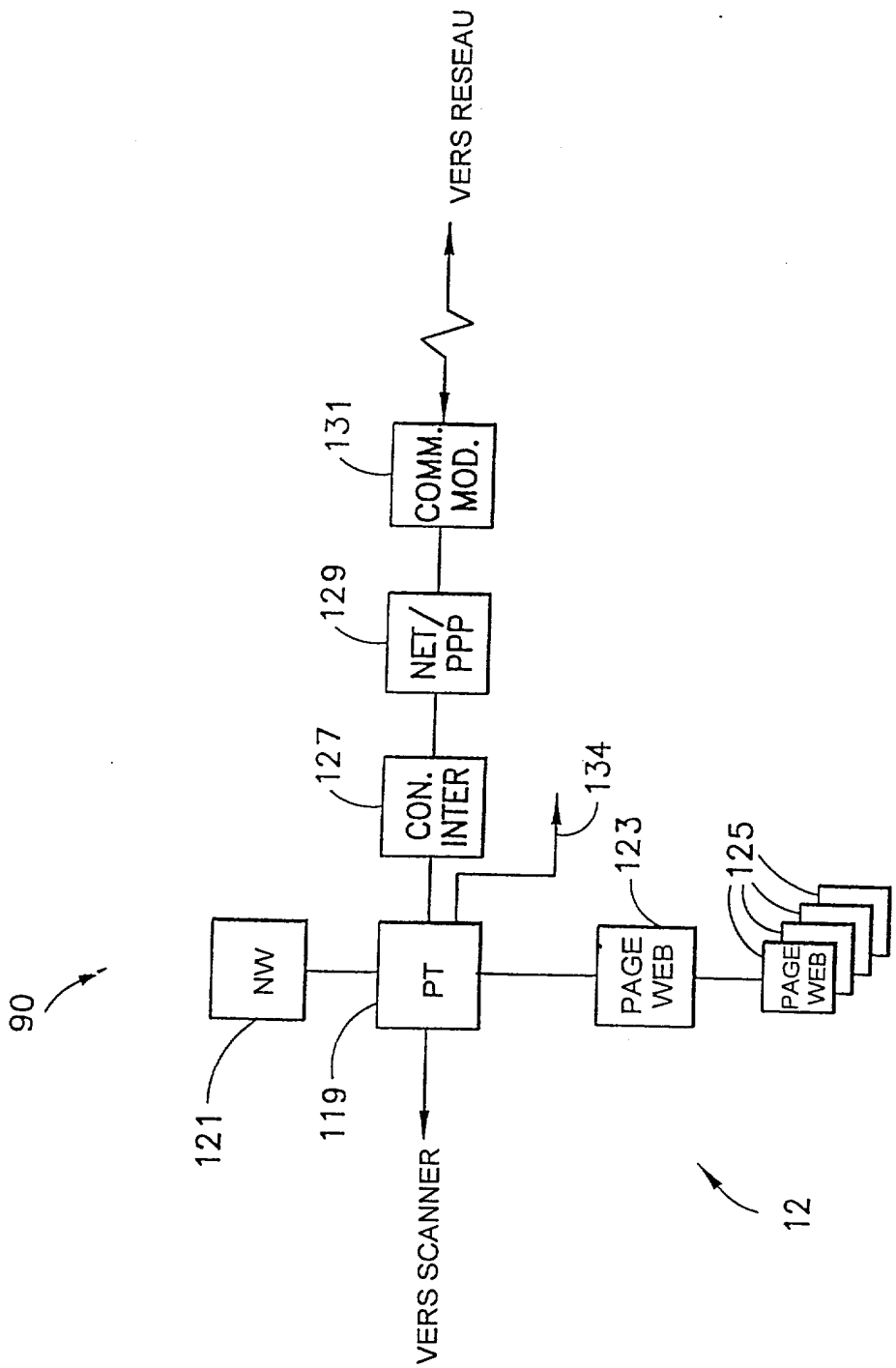

90
NW
PT
PAGE WEB
PAGE WEB
CON. INTER
NET/ PPP
COMM. MOD.
121
119
123
125
127
129
131
134
VERS SCANNER
VERS RESEAU
12

FIG.3

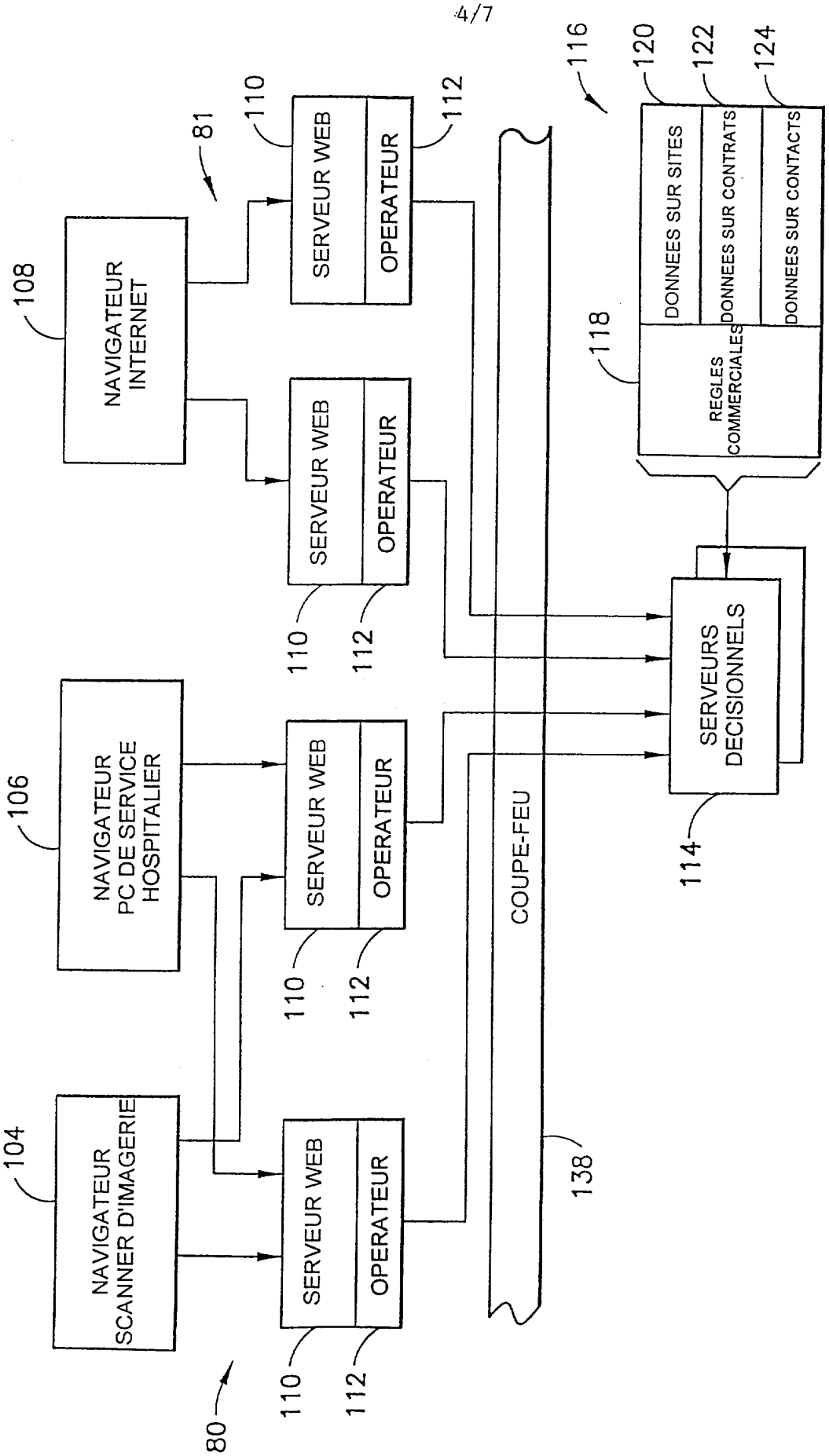

NAVIGATEUR SCANNER D'IMAGERIE
NAVIGATEUR PC DE SERVICE HOSPITALIER
NAVIGATEUR INTERNET
SERVEUR WEB
OPERATEUR
COUPE-FEU
SERVEURS DECISIONNELS
REGLES COMMERCIALES
DONNEES SUR SITES
DONNEES SUR CONTRATS
DONNEES SUR CONTACTS
GESTION DE GROUPE
80
81
104
106
108
110
112
114
116
118
120
122
124
138

FIG.4

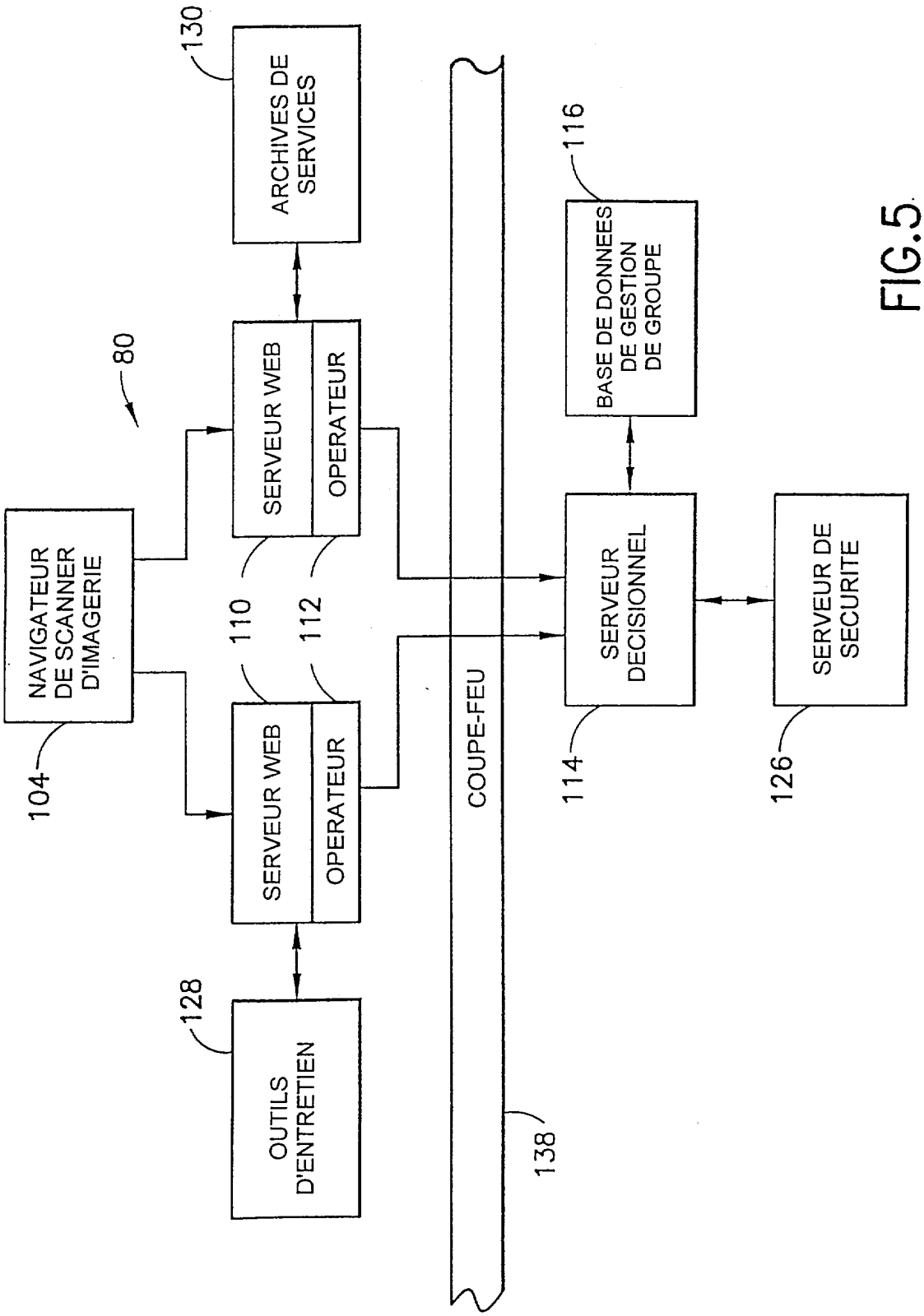

130
ARCHIVES DE SERVICES
116
BASE DE DONNEES DE GESTION DE GROUPE
80
SERVEUR WEB
OPERATEUR
NAVIGATEUR DE SCANNER D'IMAGERIE
110
112
SERVEUR DECISIONNEL
SERVEUR DE SECURITE
104
SERVEUR WEB
OPERATEUR
COUPE-FEU
114
126
128
OUTILS D'ENTRETIEN
138

FIG.5

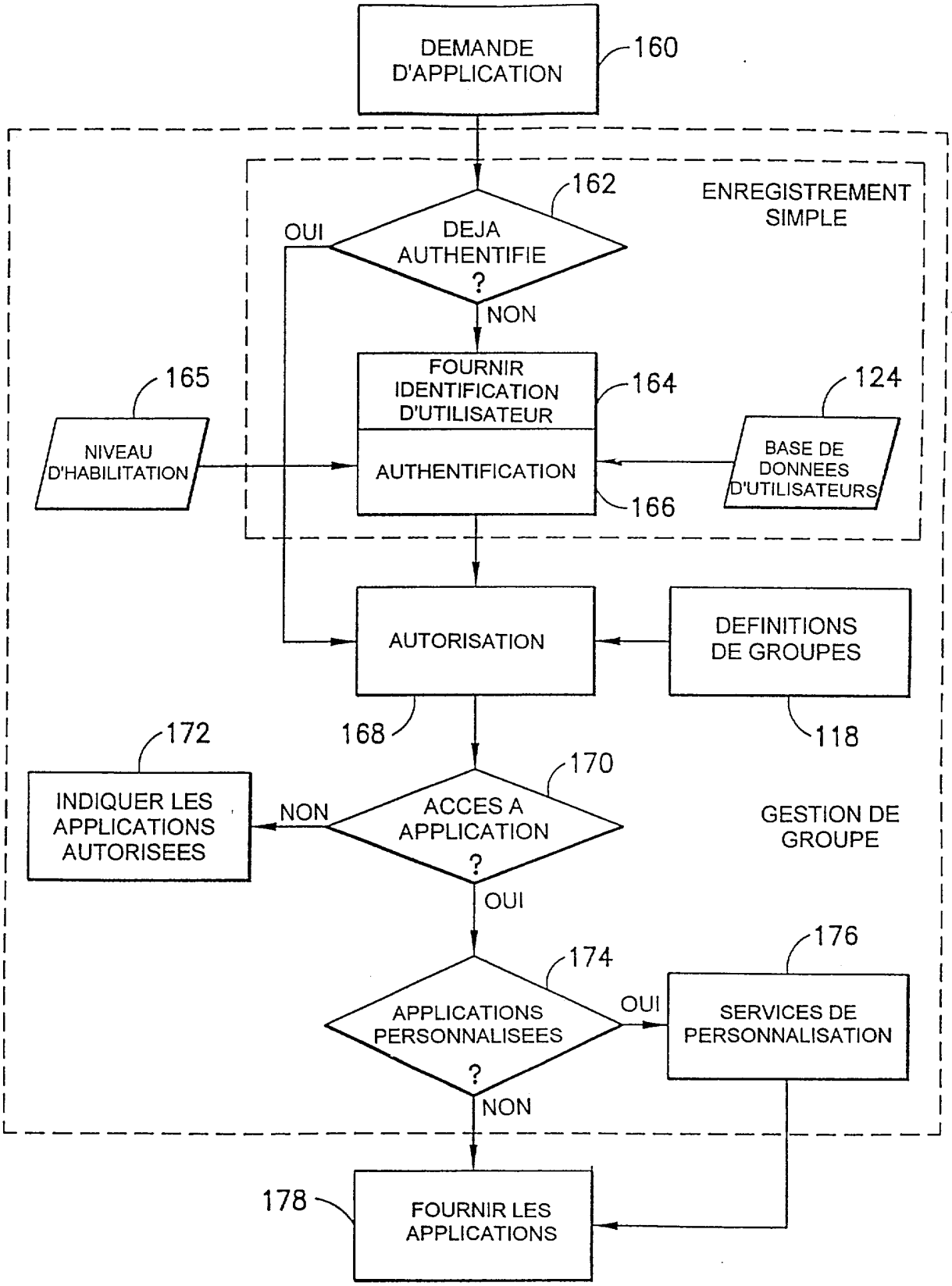

DEMANDE D'APPLICATION
160
ENREGISTREMENT SIMPLE
162
DEJA AUTHENTIFIE ?
OUI
NON
FOURNIR IDENTIFICATION D'UTILISATEUR
164
AUTHENTIFICATION
166
165
NIVEAU D'HABILITATION
124
BASE DE DONNEES D'UTILISATEURS
AUTORISATION
DEFINITIONS DE GROUPES
168
118
172
INDIQUER LES APPLICATIONS AUTORISEES
NON
170
ACCES A APPLICATION ?
GESTION DE GROUPE
OUI
174
APPLICATIONS PERSONNALISEES ?
OUI
176
SERVICES DE PERSONNALISATION
NON
178
FOURNIR LES APPLICATIONS

FIG.6

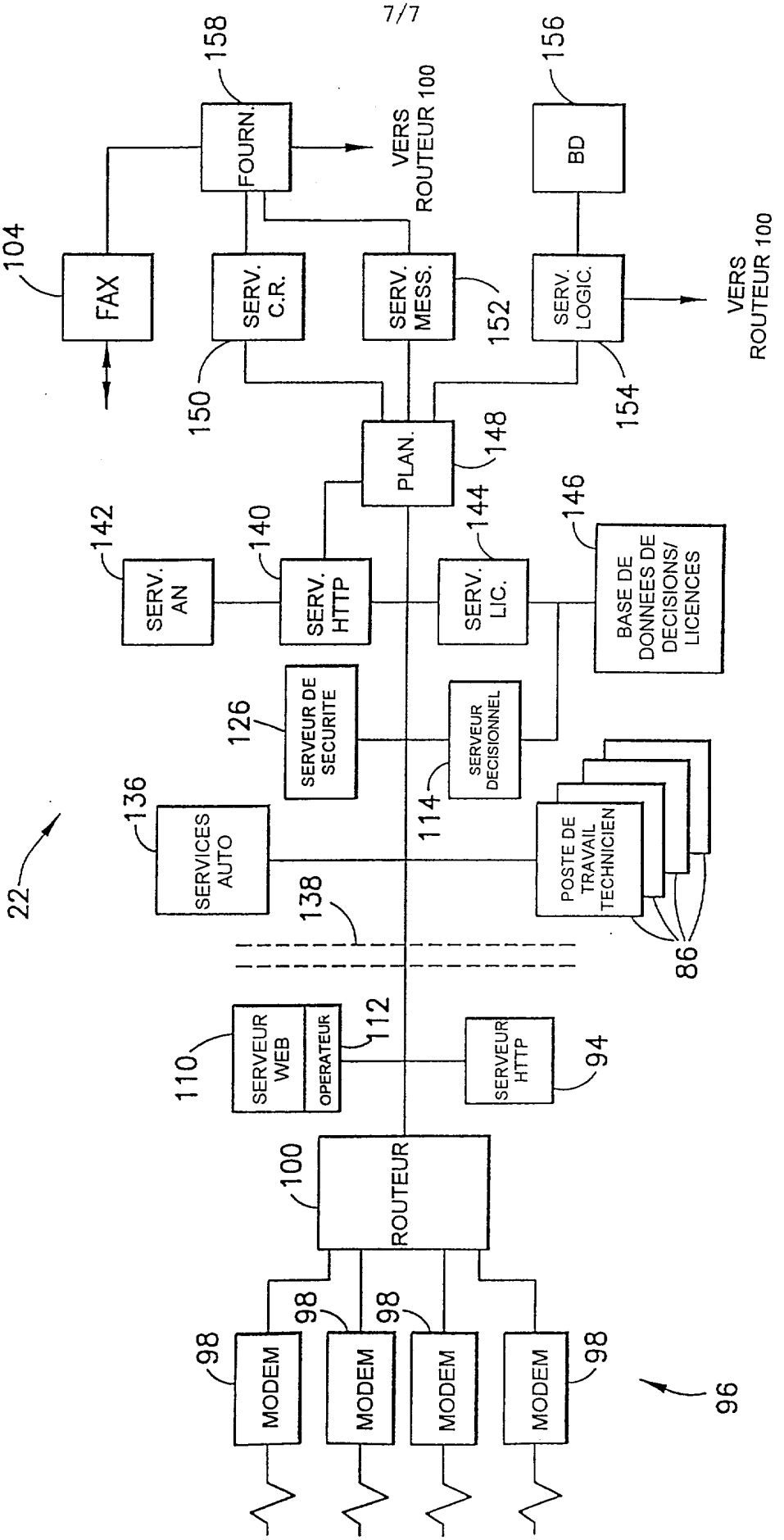

22
104
FAX
158
FOURN.
VERS ROUTEUR 100
156
BD
SERV. C.R.
150
SERV. MESS.
152
SERV. LOGIC.
154
VERS ROUTEUR 100
PLAN.
148
142
SERV. AN
140
SERV. HTTP
144
SERV. LIC.
146
BASE DE DONNEES DE DECISIONS/ LICENCES
126
SERVEUR DE SECURITE
SERVEUR DECISIONNEL
114
136
SERVICES AUTO
138
POSTE DE TRAVAIL TECHNICIEN
86
110
SERVEUR WEB
OPERATEUR
112
SERVEUR HTTP
94
100
ROUTEUR
98
MODEM
98
MODEM
98
MODEM
98
MODEM
96

FIG.7