(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 août 2002 (01.08.2002)

PCT

(10) Numéro de publication internationale
WO 02/060151 A2

(51) Classification internationale des brevets[7] : H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR02/00305

(22) Date de dépôt international :
25 janvier 2002 (25.01.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/01097 26 janvier 2001 (26.01.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 GEMENOS (FR).

(72) Inventeurs; et

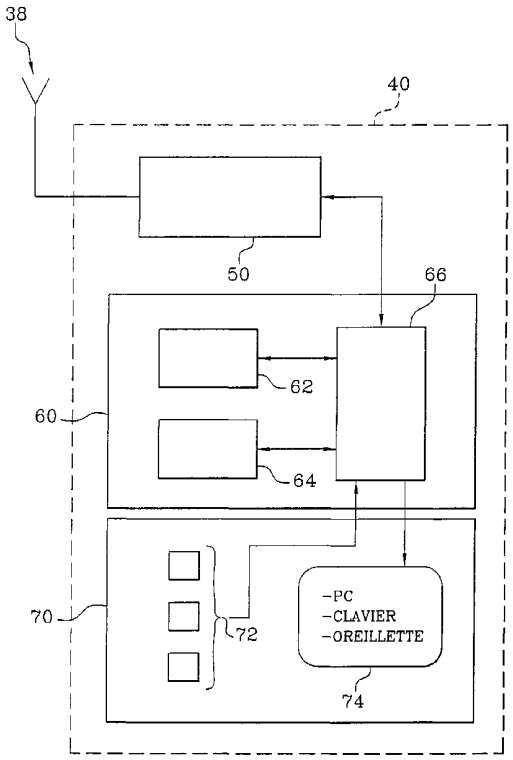
(75) Inventeurs/Déposants *(pour US seulement)* : **LAPORTE, Frédéric** [FR/FR]; 31 Blvd Joseph Vernet, F-13008 MARSEILLE (FR). **HAUSER, Jean-Luc** [FR/FR]; Résid Prado Plazza Bt B, 32, rue des Mousses, F-13008 MARSEILLE (FR). **ROSE, Murielle** [FR/FR]; 23, Impasse Olive Heimburger, Clos la Graponière, F-83390 CUERS (FR).

(74) Mandataire : **AIVAZIAN, Denis**; c/o GEMPLUS, Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 GEMENOS (FR).

[Suite sur la page suivante]

(54) Title: DEVICE AND METHOD FOR AUTOMATIC AND SECURE PAIRING A RADIOFREQUENCY NETWORK APPLIANCES

(54) Titre : DISPOSITIF ET PROCEDE D'APPAIRAGE AUTOMATIQUE SECURISE DES APPAREILS D'UN RESEAU RADIOFREQUENCE



74...PC
KEYBOARD
EAR CUSHION

(57) Abstract: The invention concerns a device for automatic and secure pairing (40) of appliances of a radiofrequency network, characterised in that it comprises a connection module (50, 38) for communicating with each of the appliances of said radiofrequency network, and an electronic pairing module (60) for providing a network appliance with a pairing key for communicating with at least another appliance of the frequency network. The invention is applicable to pairing appliances in a BLUETOOTH type network.

(57) Abrégé : L'invention concerne un dispositif d'appairage automatique et sécurisé (40) des appareils d'un réseau radiofréquence, caractérisé en ce qu'il comprend : - un module de connexion (50,38) pour communiquer avec chacun des appareils dudit réseau radiofréquence, et- un module électronique d'appairage (60) permettant de fournir à un appareil du réseau une clé d'appairage pour communiquer avec au moins un autre appareil du réseau radiofréquence.L'invention est applicable à l'appairage d'appareils dans un réseau de type BLUETOOTH.

WO 02/060151 A2

(81) États désignés *(national)* **:** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

DISPOSITIF ET PROCEDE D'APPAIRAGE AUTOMATIQUE SECURISE DES APPAREILS D'UN RESEAU RADIOFREQUENCE

L'invention concerne les réseaux radiofréquence dans lesquels les appareils d'un réseau communiquent entre eux par des liaisons radiofréquence et, plus particulièrement dans de tels réseaux, un dispositif et un procédé pour appairer entre eux de manière sécurisée et automatique les appareils du réseau.

Il est connu de réaliser des liaisons radiofréquence entre des appareils électroniques tels qu'un ordinateur personnel, une imprimante, un combiné téléphonique portable ou fixe, etc, en mettant en oeuvre, par exemple, les spécifications d'un réseau appelé "BLUETOOTH" qui sont définies dans les documents ETS 300-328 et ETS 300-339.

Dans un tel réseau BLUETOOTH, les appareils communiquent en "clair" de manière non sécurisée ou à l'aide de messages cryptés par des algorithmes symétriques à clé privée.

Cette seconde solution permet une communication sécurisée mais il se pose alors le problème de l'échange initial de la clé. Le standard BLUETOOTH propose un échange en "clair" ou l'utilisation d'un câble pour connecter les deux appareils durant cette phase d'échange de clés. Ces solutions ne sont pas satisfaisantes tant sur le plan pratique que sur celui de la sécurité.

Pour pallier ce problème, il a été proposé de rentrer manuellement la clé dans chacun des deux appareils à connecter.

Cette procédure peut s'avérer fastidieuse dans la mesure où il faut saisir deux fois ce code sur un

clavier, code qui peut avoir de nombreux chiffres et/ou lettres.

Par ailleurs, certains appareils du réseau peuvent ne pas avoir de clavier, par exemple une oreillette d'écoute d'un appareil portable téléphonique, de sorte que l'on est amené à enregistrer ce code de manière permanente ou presque dans l'appareil sans clavier.

Ceci conduit à permettre à tout porteur de l'appareil de s'introduire dans le réseau sans avoir à s'authentifier en tant que personne.

Il est aussi proposé de connecter les deux appareils par l'intermédiaire d'une liaison filaire de manière à échanger en toute sécurité les clés de session pour assurer ensuite l'authentification et le cryptage.

L'inconvénient de cette solution réside dans le fait que chaque appareil doit être équipé d'une prise spéciale qui sera différente d'un appareil à l'autre.

Dans la demande de brevet français N° 00 09774 déposée le 26 juillet 2000 par la demanderesse, il est proposé un procédé de reconnaissance sécurisée entre deux appareils d'un réseau radiofréquence qui comprend les étapes suivantes consistant à :

(a) mettre en marche les deux appareils,

(b) sélectionner l'un des deux appareils comme appareil-maître et l'autre comme appareil-esclave,

(c) approcher les deux appareils à proximité immédiate l'un de l'autre,

(d) lancer sur l'appareil-maître une procédure automatique de reconnaissance sécurisée consistant à :

(d1) émettre des signaux selon un diagramme de rayonnement tel que les signaux ne soient reçus que par l'appareil-esclave,

(d2) lancer une procédure classique de connexion au réseau radiofréquence et, en cas de succès de connexion au réseau radiofréquence,

(d3) générer une clé de reconnaissance en vue de sécuriser les échanges ultérieurs,

(d4) émettre à nouveau des signaux selon le diagramme de rayonnement habituel, et

(e) éloigner les deux appareils l'un de l'autre pour un fonctionnement à distance normale.

Les étapes (d1) et (d2) sont répétées en cas d'échec de l'étape (d2) de connexion radiofréquence. Les étapes (d1) et (d2) sont répétées au moins une fois avec un diagramme de rayonnement de portée plus grande.

Le procédé qui vient d'être décrit est satisfaisant du point de vue de la sécurité qu'il apporte mais il implique de modifier les appareils du réseau pour que leur diagramme de rayonnement soit modifiable afin que leur portée puisse être réduite à quelques centimètres pendant leur reconnaissance mutuelle.

Un but de la présente invention est donc de réaliser un dispositif dédié à l'appairage sécurisé des appareils d'un réseau radiofréquence qui ne nécessite pas de modification des appareils du réseau radiofréquence.

Par ailleurs, les procédés de l'art antérieur impliquent, de la part de l'utilisateur des appareils du réseau radiofréquence, la connaissance de codes et la manipulation de touches sur les appareils pour entrer ces codes et, éventuellement, la manipulation de fils de connexion entre les deux appareils à connecter.

Un autre but de la présente invention est donc de réaliser un dispositif dédié à l'appairage sécurisé des appareils d'un réseau radiofréquence qui permet l'appairage automatique de chaque appareil du réseau

radiofréquence au fur et à mesure des besoins de connexion.

L'invention concerne donc un dispositif d'appairage sécurisé et automatique des appareils d'un réseau informatique, caractérisé en ce qu'il comprend :

- un module de connexion pour communiquer avec chacun des appareils dudit réseau radiofréquence, et
- un module électronique d'appairage permettant de fournir à un appareil du réseau une clé d'appairage pour communiquer avec au moins un autre appareil du réseau radiofréquence.

Le dispositif selon l'invention peut comprendre, en outre, une interface Homme/Machine qui comprend au moins une touche de commande Marche/Arrêt.

Cette interface peut comprendre, en outre, un écran d'affichage pour visualiser, notamment, des informations de fonctionnement du dispositif.

Le module de connexion comprend des moyens pour limiter la portée d'émission/réception du dispositif à quelques centimètres.

Le module électronique d'appairage comprend :

- au moins une mémoire pour enregistrer au moins un code ou clé de chiffrement aux appareils à appairer, et
- un circuit de commande de la mémoire pour réaliser une procédure automatique de connexion et fournir à un appareil du réseau une clé d'appairage.

La mémoire peut être prévue pour enregistrer les différentes clés d'appairage aux appareils à appairer.

Les clés d'appairage peuvent être fournies par un générateur de clés.

L'invention concerne également un procédé d'appairage sécurisé et automatique des appareils d'un réseau radiofréquence à l'aide du dispositif décrit ci-dessus,

caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) approcher le dispositif à proximité immédiate (quelques centimètres) de l'appareil à appairer,

(b) activer le dispositif et l'appareil à appairer,

(c) fournir à l'appareil à appairer au moins une clé d'appairage pour être utilisée lors des communications avec au moins un autre appareil du réseau, et

(d) retourner à l'étape (a) pour un autre appareil à appairer.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante d'un exemple particulier de réalisation, ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 montre schématiquement un réseau radiofréquence qui connecte plusieurs appareils entre eux, et

- la figure 2 est un schéma fonctionnel simplifié d'un dispositif selon l'invention,

L'invention sera décrite dans son application à un réseau radiofréquence 80 (figure 1) réalisé et fonctionnant selon les spécifications du système précité BLUETOOTH. Ce réseau 60 est par exemple prévu pour connecter un appareil téléphonique portable 10 à une oreillette d'écoute 12 et à un ordinateur personnel 26, ce dernier étant connecté via le réseau 60 à un clavier 32.

A cet effet, les différents appareils 10, 12, 26 et 32 sont équipés d'un module BLUETOOTH 50 qui émet et reçoit des signaux radioélectriques via une antenne 14 pour l'appareil téléphonique portable, 16 pour

l'oreillette, 52 pour l'ordinateur personnel, 26 et 54 pour le clavier 32.

Dans l'état actuel du système BLUETOOTH, la connexion d'un appareil au réseau doit être effectuée selon un processus particulier qui implique des manipulations par l'utilisateur de l'appareil concerné, par exemple, en entrant un code d'accès par les touches 56 du clavier 32 ou les touches 20 de l'appareil téléphonique portable 10. D'autres touches de Marche/Arrêt 24 et de "navigation" 22 sur un écran 18 peuvent être aussi utilisées.

En l'absence de touches, sur l'appareil à connecter, il est prévu des connexions filaires, par exemple pour appairer l'oreillette 12 à l'appareil téléphonique portable 10 ou pour appairer le clavier 32 à l'ordinateur personnel 26.

C'est pendant le processus de connexion ou d'appairage au réseau que les appareils susceptibles de communiquer entre eux s'échangent des clés de reconnaissance ou d'appairage qui sont ensuite utilisées pour effectuer ultérieurement des communications de manière sécurisée.

Dans la demande de brevet précitée, il a été décrit un procédé pour sécuriser ce processus de connexion ou d'appairage entre deux appareils du réseau, par exemple entre l'oreillette 12 et l'appareil téléphonique portable 10.

L'invention propose un dispositif pour appairer de manière automatique et sécurisée chaque appareil au réseau de sorte que chaque appareil peut ensuite se connecter à un autre ou plusieurs autres appareils du réseau.

Selon l'invention, ce dispositif peut se présenter sous la forme d'une carte à puce électronique sans contact 34 ou sous toute autre forme.

Quelle que soit sa forme extérieure, ce dispositif comprend essentiellement (figures 1 et 2) :

- un module BLUETOOTH 50 associé à une antenne 38, qui comprend essentiellement des moyens d'émission/réception fonctionnant suivant les spécifications des normes précitées, et
- un module électronique d'appairage 60.

Le module BLUETOOTH peut être remplacé par un module de communication à distance équivalent tels que ceux fonctionnant par faisceau infra-rouge, par couplage magnétique ou capacitif.

Il peut également comprendre :

- une interface homme/machine 70 qui peut ou non comprendre :
- une ou plusieurs touches de commande 72,
- et/ou un écran de visualisation 74.

Le module électronique d'appairage 60 comprend :

- une mémoire 62 pour enregistrer au moins un code ou clé d'appairage,
- un circuit de commande 66 qui fournit des signaux de commande de la mémoire 62 et du module BLUETOOTH 50.

En présence de l'interface homme/machine 70, le circuit de commande reçoit des signaux des touches 72 et fournit des signaux de visualisation pour l'affichage sur l'écran 74.

La mémoire 62 peut être remplacée ou complétée par un générateur de clés 64.

Le module électronique d'appairage 60 est de préférence réalisé par un microcontrôleur et ses mémoires associées mettant en oeuvre des programmes spécifiques,

notamment pour effectuer des calculs cryptographiques et contrôler le processus d'appairage.

Le module BLUETOOTH et, plus particulièrement, les moyens d'émission/réception sont calibrés pour avoir un diagramme de rayonnement dont la portée n'est que de quelques centimètres.

Si le dispositif selon l'invention est du type sans contact, l'énergie électrique pour son fonctionnement doit lui être fournie soit par une pile électrique, soit par l'énergie haute fréquence reçue de l'appareil à appairer à l'aide d'un circuit de redressement et filtrage de type classique.

Le dispositif selon l'invention doit être mis en oeuvre selon les étapes suivantes consistant à :

(a) approcher le dispositif 40 à proximité immédiate (quelques centimètres) de l'appareil à appairer 10, 12, 26 ou 32,

(b) activer le dispositif 40 et l'appareil à appairer 10, 12, 26 ou 32,

(c) fournir à l'appareil à appairer 10, 12, 26 ou 32 au moins une clé d'appairage pour être utilisée lors des communications avec un autre appareil du réseau, et

(d) retourner à l'étape (a) pour un autre appareil à appairer.

La procédure de reconnaissance entre le dispositif 40 et l'appareil à appairer consiste essentiellement à comparer des clés fournies par le dispositif 40 et l'appareil à appairer et à déterminer qu'ils sont autorisés à communiquer entre eux en cas de comparaison positive.

Les clés à comparer peuvent être contenues dans la mémoire 62 du dispositif ou dans une mémoire semblable

de l'appareil à appairer ; elles peuvent aussi être calculées grâce au générateur de clés 64 ou à un circuit de calcul semblable de l'appareil à appairer.

Ces clés d'appairage, qui permettent de reconnaître que l'appareil à appairer est autorisé à être connecté au réseau radiofréquence de l'utilisateur du dispositif 40, sont différentes de la clé qui est utilisée pour sécuriser les communications entre les appareils à appairer (étape(d)). Les étapes (a) et (b) sont effectuées par l'utilisateur du dispositif 40 tandis que les étapes (c) et (d) sont effectuées par le dispositif 40 sous la commande du circuit 66.

L'interface Homme/Machine 70 permet à l'utilisateur par les touches 72 d'être l'initiateur de certaines étapes telles que les étapes (a) et (b) ou d'être renseigné, par l'écran 74, sur les étapes effectuées ou en cours, ou sur l'identité de l'appareil à appairer, en cours d'appairage ou déjà appairé.

Cependant, cette interface Homme/Machine peut être réduite à une seule touche de commande pour activer le dispositif 40 (étape (b)), les étapes suivantes étant effectuées automatiquement par le dispositif 40.

Le dispositif 40 est prévu pour initialiser tous les appareils que l'utilisateur est susceptible d'utiliser dans le réseau radiofréquence et, de ce fait, il dispose dans la mémoire 62 de toutes les clés d'appairage affectées à chaque appareil à appairer.

La mémoire 62 peut aussi contenir, outre les clés d'appairage, des paramètres de configuration de l'appareil à appairer qui lui sont transmis lors de son démarrage initial après sa livraison chez l'utilisateur. Ces paramètres ou certains d'entre eux

peuvent aussi être retransmis à l'appareil à appairer à chaque mise en réseau selon le procédé de l'invention.

Le dispositif selon l'invention comporte de préférence un jeu de clés pour permettre différents appairages ou un générateur de clés. Ce dispositif peut comprendre également des moyens d'actionnement pour changer de clés à partager entre les différents appareils, tels que touches, clavier ou autres.

Le dispositif réalise un stockage des clés. Lors de son utilisation, il est approché des appareils destinés à communiquer ensemble pour leur fournir une clé commune.

Le dispositif comprend aussi des moyens 66 pour gérer les différentes clés, notamment pour les affecter à chaque appareil soit sur intervention de l'utilisateur à l'aide d'un clavier, soit de manière automatique en l'associant à l'identifiant de l'appareil.

Lors de la transmission de la clé, le dispositif peut recevoir de l'appareil ses caractéristiques qui sont mémorisées en les associant avec un identifiant de la clé pour permettre une gestion des clés.

Le dispositif et le procédé selon l'invention présentent les avantages suivants :

- l'appareil à appairer n'a pas besoin d'adaptation particulière telle qu'un lecteur de carte à puce, de fils de connexion, ou de touche de commande particulière pour être connecté au réseau ;
- l'utilisateur du dispositif n'a pas besoin de connaître un ou plusieurs codes d'accès car ils sont contenus dans la mémoire 62 ;
- l'appareil à appairer est configuré selon des caractéristiques enregistrées dans la mémoire 62, donc sans intervention de l'utilisateur, sauf s'il souhaite les modifier ;

- les informations et paramètres personnels de l'utilisateur sont enregistrés dans la mémoire 62 et sont protégés contre toute fraude ;
- l'appairage s'effectue de manière automatique et sécurisée avec une intervention minimale de l'utilisateur.

REVENDICATIONS

1. Dispositif d'appairage automatique et sécurisé (40) des appareils d'un réseau radiofréquence, caractérisé en ce qu'il comprend :
- un module de connexion (50, 38) pour communiquer avec chacun des appareils dudit réseau radiofréquence, et
- un module électronique d'appairage (60) permettant de fournir à un appareil du réseau (10, 12, 26 ou 32) une clé d'appairage pour communiquer avec au moins un autre appareil du réseau radiofréquence.

2. Dispositif selon la revendication 1, caractérisé en ce que le module de connexion comprend des moyens pour limiter la portée dudit module de connexion.

3. Dispositif selon la revendication 2, caractérisé en ce que le module de connexion (50, 38) est du type radiofréquence lui permettant de se connecter audit réseau radiofréquence.

4. Dispositif selon la revendication 1, 2 ou 3, caractérisé en ce qu'il comprend, en outre, une interface Homme/Machine (70) comprenant au moins une touche de commande (72) de Marche/Arrêt dudit dispositif.

5. Dispositif selon la revendication 4, caractérisé en ce que l'interface Homme/Machine (70) comprend, en outre, un écran d'affichage (74).

6. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que le module électronique d'appairage (60) comprend :

- au moins une mémoire (62) pour enregistrer au moins un code ou clé de chiffrement aux appareils à appairer, et

- un circuit de commande (66) de la mémoire (62) pour réaliser la procédure automatique de connexion et fournir à un appareil du réseau une clé d'appairage.

7. Dispositif selon la revendication 6, caractérisé en ce que la mémoire (62) est prévue pour enregistrer les différentes clés d'appairage aux appareils à appairer.

8. Dispositif selon la revendication 6 ou 7, caractérisé en ce que la mémoire (62) est prévue pour enregistrer les différentes caractéristiques de l'appareil récepteur d'une clé d'appairage.

9. Dispositif selon l'une des revendications 6 à 9, caractérisé en ce que la mémoire 62 est prévue pour enregistrer les différentes configurations des appareils susceptibles d'être appairés par ledit dispositif.

10. Dispositif selon l'une des revendications 6 à 9, caractérisé en ce que la clé de chiffrement est fournie par un générateur de clés de chiffrement.

11. Dispositif selon l'une des revendications 6 à 10, caractérisé

en ce qu'il comprend des moyens (64, 66) pour changer les clés d'appairage des appareils.

12. Dispositif selon l'une des revendications 6 à 11, caractérisé en ce qu'il comprend des moyens (66) pour gérer l'affectation des clés aux divers appareils.

13. Dispositif selon l'une des revendications précédentes 1 à 12, caractérisé en ce que le module électronique d'appairage (60) est un microcontrôleur.

14. Objet portable contenant un dispositif selon l'une quelconque des revendications 1 à 13, caractérisé en ce qu'il se présente sous la forme d'une carte à puce électronique.

15. Procédé d'appairage automatique et sécurisé, des appareils d'un réseau radiofréquence à l'aide d'un dispositif ou objet selon l'une des revendications précédentes 1 à 14, caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) approcher le dispositif (40) à proximité immédiate (quelques centimètres) de l'appareil à appairer (10, 12, 26 ou 32),

(b) activer le dispositif (40) et l'appareil à appairer (10, 12, 26 ou 32),

(c) fournir à l'appareil à appairer (10, 12, 26 ou 32) au moins une clé d'appairage pour être utilisée lors de communications avec au moins un des appareils du réseau, et

(d) retourner à l'étape (a) pour un autre appareil à appairer.

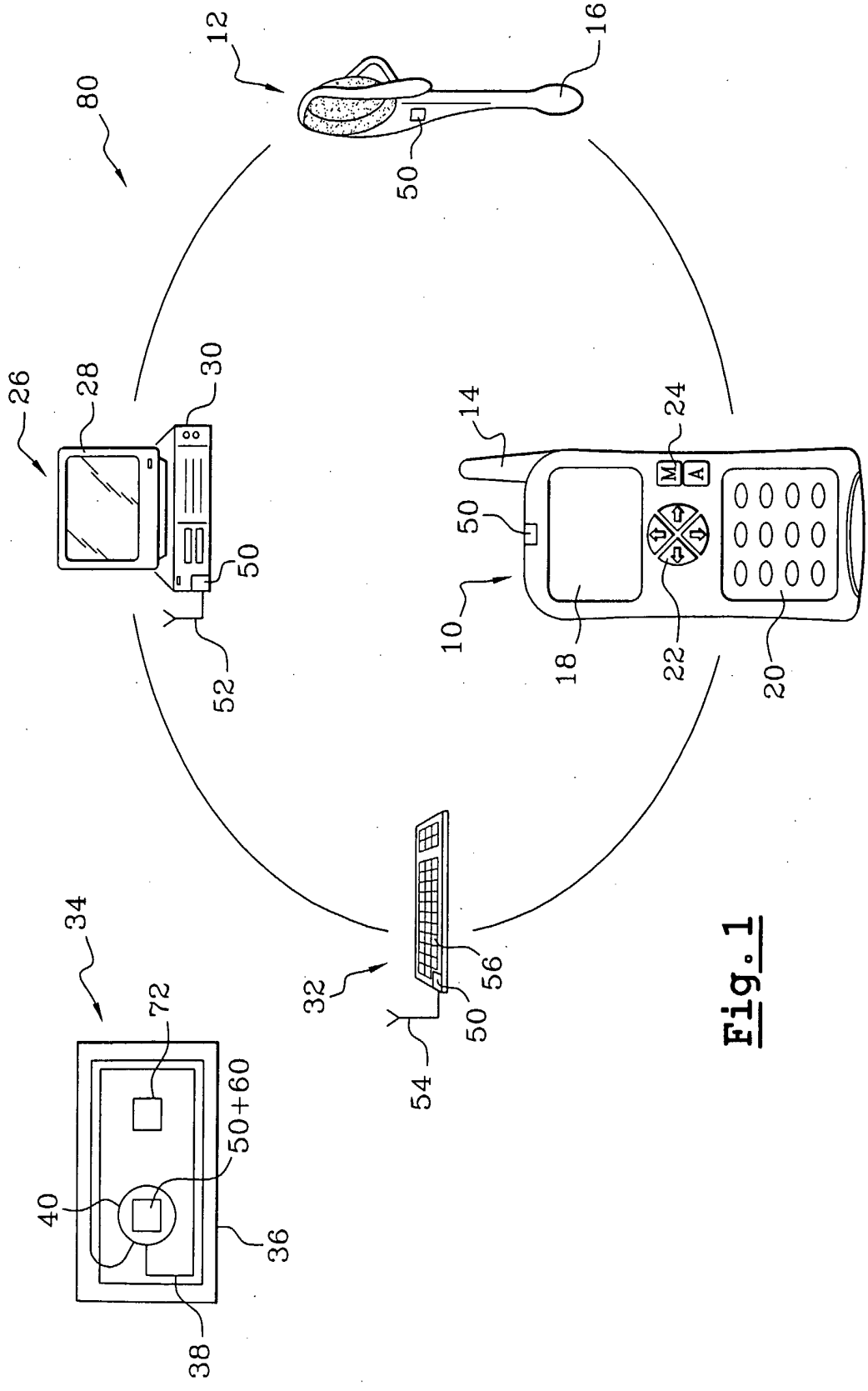

80
12
16
50
26
28
30
50
52
14
24
M
A
50
10
18
22
20
34
72
50+60
40
36
38
32
50
56
54

Fig.1

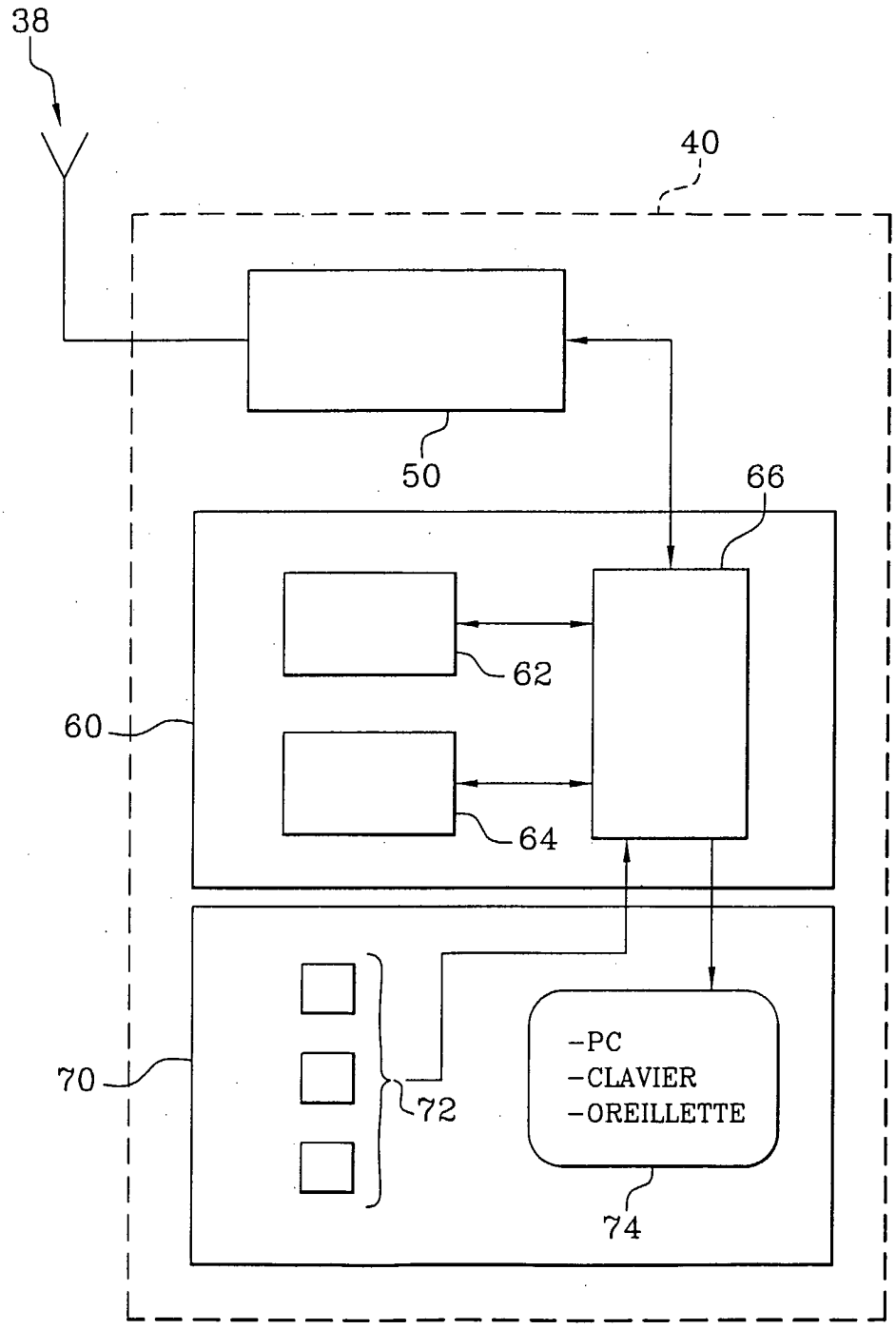


Fig. 2