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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 juillet 2003 (03.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/053739 A2

(51) Classification internationale des brevets[7] : B60Q 11/00

(21) Numéro de la demande internationale :
PCT/FR02/04431

(22) Date de dépôt international :
18 décembre 2002 (18.12.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/16579 20 décembre 2001 (20.12.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13420 Gemenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **LEDUC, Michel** [FR/FR]; 27, Lot Cabassude, F-13530 Trets (FR).

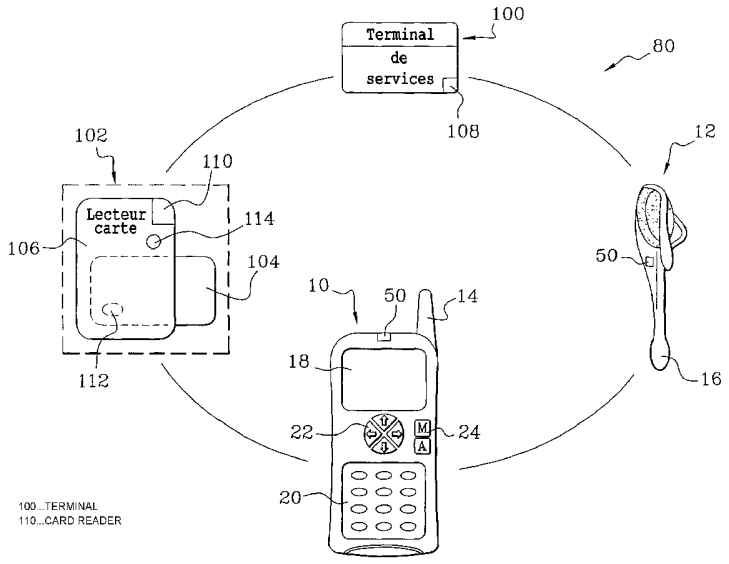
(74) Mandataire : **AIVAZIAN, Denis**; c/o Gemplus / La Vigie, Zone Athélia IV, Avenue du Jujubier, Boîte postale 90, F-13705 La Ciotat Cedex (FR).

(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, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) **Title:** METHOD FOR ACCESSING A SERVICE BY RADIOFREQUENCY MEANS ASSOCIATED WITH A MICROCHIP PORTABLE OBJECT

(54) **Titre :** PROCEDE D'ACCES A UN SERVICE PAR UN MOYEN RADIOFREQUENCE ASSOCIE A UN OBJET PORTABLE A PUCE ELECTRONIQUE



(57) **Abstract:** The invention concerns a method for identifying a user of a microchip portable object (102, 104, 106) characterized in that it comprises the following steps which consist in: providing a secure communication network (80) between the microchip portable object and at least a service terminal (100), any one of the network (80) apparatuses designed to perform a sensitive operation; setting up a first communication between the portable object (102, 104, 106) and said at least service terminal (100); setting up a second communication between the portable object (102, 104, 106) and said any one apparatus of the network (10) to perform thereon said sensitive operation; validation of the sensitive operation by the microchip portable object, and transmitting the validation result to the service terminal (100).

[Suite sur la page suivante]

WO 03/053739 A2

(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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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.

(57) Abrégé : L'invention concerne un procédé d'identification d'un utilisateur d'un objet portable ô puce électronique (102, 104, 106) caractérisé en ce qu'il comprend les étapes suivantes consistant ô :réaliser un réseau de communication sécurisé (80) entre l'objet portable ô puce électronique et au moins un terminal de services (100) l'un quelconque des appareils du réseau (80) permettant d'effectuer une opération sensible,- établir une première communication entre l'objet portable (102, 104, 106) et ledit au moins terminal de services (100),- établir une deuxième communication entre l'objet portable (102, 104, 106) et ledit quelconque appareil du réseau (10) pour effectuer sur ce dernier ladite opération sensible,,- valider l'opération sensible par l'objet portable ô puce électronique, et- transmettre le résultat de la validation au terminal de services (100).

PROCEDE D'ACCES A UN SERVICE PAR UN MOYEN RADIOFREQUENCE ASSOCIE A UN OBJET PORTABLE A PUCE ELECTRONIQUE

L'invention concerne le domaine des réseaux radiofréquence du type connu sous les acronymes "PLAN " pour l'expression anglo-saxonne "Personal Loca Area Network" tel que le réseau appelé "BLUETOOTH" et "WLAN" pour l'expression anglo-saxonne "Wireless Local Area Network" tel que celui défini par la norme 802-11 et, plus particulièrement dans ce domaine un procédé pour accéder par un moyen radiofréquence à un service à l'aide d'un objet portable comprenant une puce électronique.

Il est connu de réaliser des liaisons de communication 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 du réseau appelé "BLUETOOTH" qui sont définies dans les documents ETS 300-328 et ETS-300-339.

La figure 1 montre schématiquement un réseau radiofréquence 80 qui connecte un appareil téléphonique portable 10 (ou station mobile) à une oreillette 12 et à un ordinateur personnel 26, ce dernier étant connecté via le réseau 80 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 10, 16 pour l'oreillette 12, 52 pour l'ordinateur personnel 26, 54 pour le clavier 32.

Le réseau radiofréquence 80 peut aussi comprendre d'autres appareils tels qu'un terminal de services bancaires qui permet de réaliser des opérations bancaires, par exemple le retrait d'argent liquide à l'aide d'une carte bancaire classique.

Pour que cette opération bancaire puisse s'effectuer par le réseau BLUETOOTH à l'aide de la carte bancaire, il faut que cette carte puisse communiquer de manière sécurisée avec le terminal bancaire, pour réaliser certaines actions sensibles condidentielles nécessitant une importante sécurité avant l'autorisation de l'accès en service telle l'identification d'un utilisateur par son code personnel via un clavier.

En plus des problèmes de sécurité s'ajoutent des problèmes d'infrastructure et de convivialité ; en effet, il faut un moyen d'identification tel un clavier pour rélaiser la saisie d'un code personnel et propose une manière conviviale de le faire.

Une solution à ce problème serait d'utiliser un lecteur de carte simplifié portable avec clavier et écran dans lequel serait introduite la carte bancaire de manière quasi-permanente, ce lecteur de carte étant équipé d'un module BLUETOOTH pour se connecter au terminal de services via le réseau BLUETOOTH.

Une telle solution présente l'inconvénient d'utiliser un nouvel appareil ayant un volume et un poids conséquents qu'il faudrait sortir de sa poche et en manipuler les touches du clavier pour effectuer une opération avec le terminal de services.

La présente invention propose de réaliser, dans un réseau radiofréquence sécurisé, des opérations entre une carte à puce électronique portée par un lecteur de carte et un terminal de services via un autre appareil

du réseau muni d'un élément d'identification tel qu'un clavier pour tabuler un code d'identification ou une touche d'identification.

Cet autre appareil du réseau est, par exemple, le téléphone mobile personnel de l'utilisateur de la carte à puce électronique, un terminal de paiement portable ou une borne Internet.

L'invention concerne donc un procédé d'accès à un service à l'aide d'un objet portable à puce électronique caractérisé en ce qu'il comprend les étapes suivantes consistant à :

- réaliser un réseau de communication sécurisé entre l'objet portable, à puce électronique et au moins un terminal de services, l'un quelconque des appareils du réseau permettant d'effectuer une opération sensible,
- établir une première communication entre l'objet portable et ledit au moins terminal de services,
- établir une deuxième communication entre l'objet portable et ledit quelconque appareil du réseau pour effectuer sur ce dernier ladite opération sensible,
- valider l'opération sensible par l'objet portable à puce électronique, et
- transmettre le résultat de la validation au terminal de services.

L'opération sensible est réalisée par un troisième appareil dit de saisie, la saisie consistant en un élément d'identification tel q'un code personnel.

L'objet protable est une carte à puce électronique équipé d'un moyen de communication pour se connecter en réseau de communication sécurisé. Il faut aussi comprendre une carte à puce électronique associée à un

lecteur de carte à puce qui est équipé d'un moyen de communication pour se connecter en réseau de communicatijon sécruisé. L'appareil de saisie est un appareil connecté en réseau de communication sécurisé qui comprend des moyens pour saisir un élément d'identification.

Les moyens de saisie d'un élément d'identification comprennent un clavier ou une touche pour saisir l'élément d'identification, l'élément d'identification pouvant être du type biométrique.

Le lecteur de carte à puce comprend une touche marche/arrêt pour permettre la conversion ou non du lecteur en réseau de communication sécurisé. Le lecteur peut comprendre un logiciel applicatif pour permettre la connexion automatique du lecteur en réseau de communication sécurisé.

Le logiciel applicatif de connexion automatique est apte à gérer les choix, préférences et autorisation de l'utilisateur de l'objet portable.

L'invention concerne également un lecteur de carte à puce, une carte à puce ou une carte SIM, apte à mettre en oeuvre le procédé de l'invention.

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 du type BLUETOOTH qui connecte plusieurs appareils entre eux, et
- la figure 2 est un schéma d'un réseau radiofréquence du type BLUETOOTH auquel s'applique le procédé selon l'invention.

L'invention sera décrite dans le cadre d'un réseau de communication du type BLUETOOTH selon le schéma de la figure 1 décrite dans le préambule. Cependant, elle s'applique à d'autres types de réseau de communication tels que ceux cités dans le préambule.

Dans la figure 2, les éléments identiques à ceux de la figure 1 portent des références identiques et concernent l'appareil téléphonique portable 10, encore appelé station mobile, ainsi que l'oreillette 12.

Les éléments nouveaux sont un terminal de services 100 et un objet portable 102 comprenant une carte à puce électronique 104 insérée dans un lecteur de carte 106.

Le terminal de services 100 est par exemple un terminal d'opérations bancaires tel qu'un distributeur de billets de banque pour des retraits d'argent liquide ou tout autre type de terminal apte à fournir au moins un service sur présentation de la carte à puce électronique dans un lecteur de carte associé au terminal. Un tel terminal peut être équipé d'un écran et d'un clavier en tant qu'interface homme/machine.

A titre d'exemples de terminaux de services seront également cités les appareils de paiement par carte bancaire utilisés par les commerçants pour effectuer une transaction de paiement.

Pour mettre en oeuvre l'invention, ce terminal de services est équipé d'un module d'émission/réception BLUETOOTH 108 qui lui permet de s'intégrer dans le réseau 80.

La carte à puce électronique 104, qui est habituellement utilisée dans le lecteur de carte associé au terminal 100, est associée de manière quasi-permanente au lecteur de carte 106 par l'intermédiaire de contacts électriques 112. Ce lecteur de carte 106

est de type simplifié, sans écran et sans clavier, mais comprend un module d'émission/réception BLUETOOTH 110 ainsi qu'une touche de marche/arrêt 114. L'énergie électrique est fournie par une pile (non représentée).

Le procédé selon l'invention consiste à autoriser l'accès à un service proposé par le terminal 100 via le lecteur de carte 106 et la station mobile 10 en utilisant l'écran 18 et le clavier 20 de la station mobile pour dialoguer avec le terminal 100, notamment pour fournir un élément d'identification tel qu'un code d'accès au service.

La station mobile 10 peut être remplacée par tout autre appareil équipé d'un clavier ou d'une touche d'identification, pour fournir l'élément d'identification d'accès au service.

Les étapes du procédé seront maintenant décrites en supposant que l'appareil mobile 10, l'oreillette 12, le terminal 100 et 102 sont connectés au réseau 80 de façon sécurisée selon un procédé de reconnaissance sécurisée.

Un procédé pour établir une communication sécurisée entre par exemple la station mobile 10 et l'oreillette 12, comprend les étapes suivantes consistant à :

(a) mettre en marche les deux appareils (10, 12),

(b) sélectionner l'un (10) des deux appareils comme appareil-maître et l'autre (12) comme appareil-esclave,

(c) approcher les deux appareils (10, 12) à proximité immédiate l'un de l'autre,

(d) lancer sur l'appareil-maître (10) 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 (12),

(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 (10, 12) l'un de l'autre pour un fonctionnement à distance normale.

Lorsque l'utilisateur de la carte à puce 104 souhaite bénéficier d'un ou plusieurs services offerts par le terminal 100, il appuie sur la touche marche/arrêt 114 du lecteur de carte 106. Cette manipulation de la touche 112 déclenche l'établissement d'une communication entre le lecteur de carte 106 et le terminal 100 via le réseau 80. Ce dernier requiert à la carte à puce 104 via le lecteur de carte 106 une identification de l'utilisateur, par exemple par la tabulation d'un code personnel.

Dans une variante, l'invention propose que cette initialisation du dialogue par la manipulation volontaire de la touche marche/arrêt 114 soit remplacée par une initialisation automatique réalisée par le système. A cet effet, le lecteur de carte 106 est toujours en veille et est activé par le système en utilisant un lecteur de carte comprenant, par exemple, une couche logicielle applicative qui présente des choix ou préférences telles que l'activation automatique du lecteur uniquement devant un distributeur bancaire d'une banque particulière. Cette

couche logicielle peut aussi présenter des autorisations pour des transactions automatiques par rapport à un service telles que l'accès à un transport, à un local, ...

Cette requête est transmise à l'appareil de téléphone mobile 10 via le réseau 80. L'utilisateur de cet appareil de téléphone mobile, qui est en même temps celui de la carte à puce 104, tabule son code personnel sur le clavier 20 et le transmet à la carte à puce 104 via le lecteur 106.

La carte à puce 104 valide ou non ce code personnel et transmet le résultat de la validation au terminal de services 100 via le lecteur de carte 106.

Si le résultat de la validation est négatif, le terminal de services 100 ne fournit pas le service demandé. Si le résultat de la validation est positif, le terminal de services fournit le service demandé.

Au lieu de tabuler un code personnel sur le clavier 20, une autre solution consiste à utiliser une touche d'analyse biométrique sur l'appareil de téléphonie mobile 10, les résultats de l'analyse étant transmis à la carte à puce 104 via le lecteur de carte 106.

L'identification de l'utilisateur a été décrite en détail à titre non limitatif comme un exemple d'action ou d'opération sensible à réaliser avant d'autoriser l'accès à un service. On puet citer comme autre exemple la transmission par le terminal de service du montant d'une transaction sur l'écran de l'appaiel 10 puis en retour la transmission de l'accord par l'utilisateur de ce montant.

L'appareil de saisie de l'élément d'identification peut comprendre un logiciel applicatif spécifique pour réaliser les opérations sensibles. Avantageusement, ce

logiciel sera incorporé dans un module de sécurité de type carte à puce, par exemple la carte SIM de l'appareil de téléphonie mobile.

Dans l'exemple décrit en relation avec la figure 2, c'est l'utilisateur de la carte à puce qui déclenche la mise en marche du système en manipulant la touche marche/arrêt 114 mais cette mise en marche peut avoir pour origine le terminal de services 100.

La mise en oeuvre du procédé selon l'invention requiert l'utilisation

- d'un terminal de services 100 équipé d'un module BLUETOOTH 108, par exemple,
- d'un appareil de téléphonie mobile 10 équipé d'un module BLUETOOTH 50,
- d'un lecteur de carte 106, équipé d'un module BLUETOOTH 110, dans lequel est introduite la carte à puce 104 appartenant à l'utilisateur de l'appareil de téléphonie mobile.

Ce procédé ne requiert donc pas l'utilisation d'un nouvel appareil dont la manipulation serait à maîtriser mais simplement l'utilisation d'un lecteur de carte à puce rudimentaire sans clavier, ni écran.

En outre, l'encombrement du lecteur de carte est faible et permet donc de le garder dans une poche ou un portefeuille avec une carte à puce en position de connexion avec le lecteur.

L'invention a été décrite dans le cadre d'un réseau BLUETOOTH mais elle peut être mise en oeuvre dans différents types de réseau par exemple ceux identifés ci-dessus par les acronymes "PLAN" et "WLAN".

L'appariel de saisie de l'élément d'identification peut être soit l'objet portable ou son lecteur, soit le terminal de services, ce qui constitue un avantage de

souplesse de l'invention par sa facilité de transport et son adaptabilité et un avantage de convivialité.

REVENDICATIONS

1. Procédé d'accès à un service à l'aide d'un objet portable à puce électronique (102, 104, 106) caractérisé en ce qu'il comprend les étapes suivantes consistant à :

- réaliser un réseau de communication sécurisé (80) entre l'objet portable à puce électronique et au moins un terminal de services (100) l'un quelconque des appareils du réseau (80) permettant d'effectuer une opération sensible,
- établir une première communication entre l'objet portable (102, 104, 106) et ledit au moins terminal de services (100),
- établir une deuxième communication entre l'objet portable (102, 104, 106) et ledit quelconque appareil du réseau (10) pour effectuer sur ce dernier ladite opération sensible,,
- valider l'opération sensible par l'objet portable à puce électronique, et
- transmettre le résultat de la validation au terminal de services (100).

2. Procédé selon la revendication 1, caractérié en ce que l'opération sensible est réalisée par un troisième appareil dit de saisie.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que l'opération sensible est une saisie d'un élément d'identification.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que l'objet (102) est une carte à puce

électronique (104) associée à un lecteur de carte à puce électronique (106) qui est équipé d'un moyen de communication pour se connecter au réseau de communication.

5. Procédé selon l'une des revendications 2 à 4, caractérisé en ce que l'appareil de saisie est un appareil connecté au réseau de communication sécurisé qui comprend des moyens pour saisir un élément d'identification.

6. Procédé selon la revendication 5, caractérisé en ce que l'appareil de saisie est un appareil personnel (10) du porteur de l'objet portable mettant en oeuvre des moyens (18, 20) pour saisir ledit élément d'identification.

7. Procédé selon la revendication 6, caractérisé en ce que les moyens pour saisir ledit élément d'identification comprennent un clavier (20) ou une touche pour saisir l'élément d'identification.

8. Procédé selon la revendication 7, caractérisé en ce que la touche pour saisir l'élément d'identification est du type biométrique.

9. Procédé selon l'une des revendications 4 à 8, caractérisé en ce que le lecteur de carte à puce électronique (106) comprend une touche marche/arrêt (114) pour permettre la connexion ou non du lecteur (106) au réseau de communication sécurisé.

10. Procédé selon l'une des revendications 4 à 8, caractérisé en ce que le lecteur de carte à puce électronique (106) comprend un logiciel applicatif pour permettre la connexion automatique du lecteur (106) au réseau de communication sécurisé.

11. Procédé selon la revendication 10, caractérisé en ce que le logiciel applicatif de connexion automatique est apte à gérer les choix, préférences et autorisations de l'utilisateur de l'objet portable.

12. Lecteur de carte à puce électronique (106) pour mettre en oeuvre le procédé selon l'une des revendications 4 à 11

13. Carte à puce électronique (104) avec moyen de communication pour se connecter en réseau de communication pour mettre en oeuvre le procédé selon l'une des revendicatjions 1 à 11.

14. Carte SIM d'un appareil de téléphonie mobile comprenant un logiciel applicatif pour réaliser les opérations sensibles selon le procédé des revendications 1 à 11.

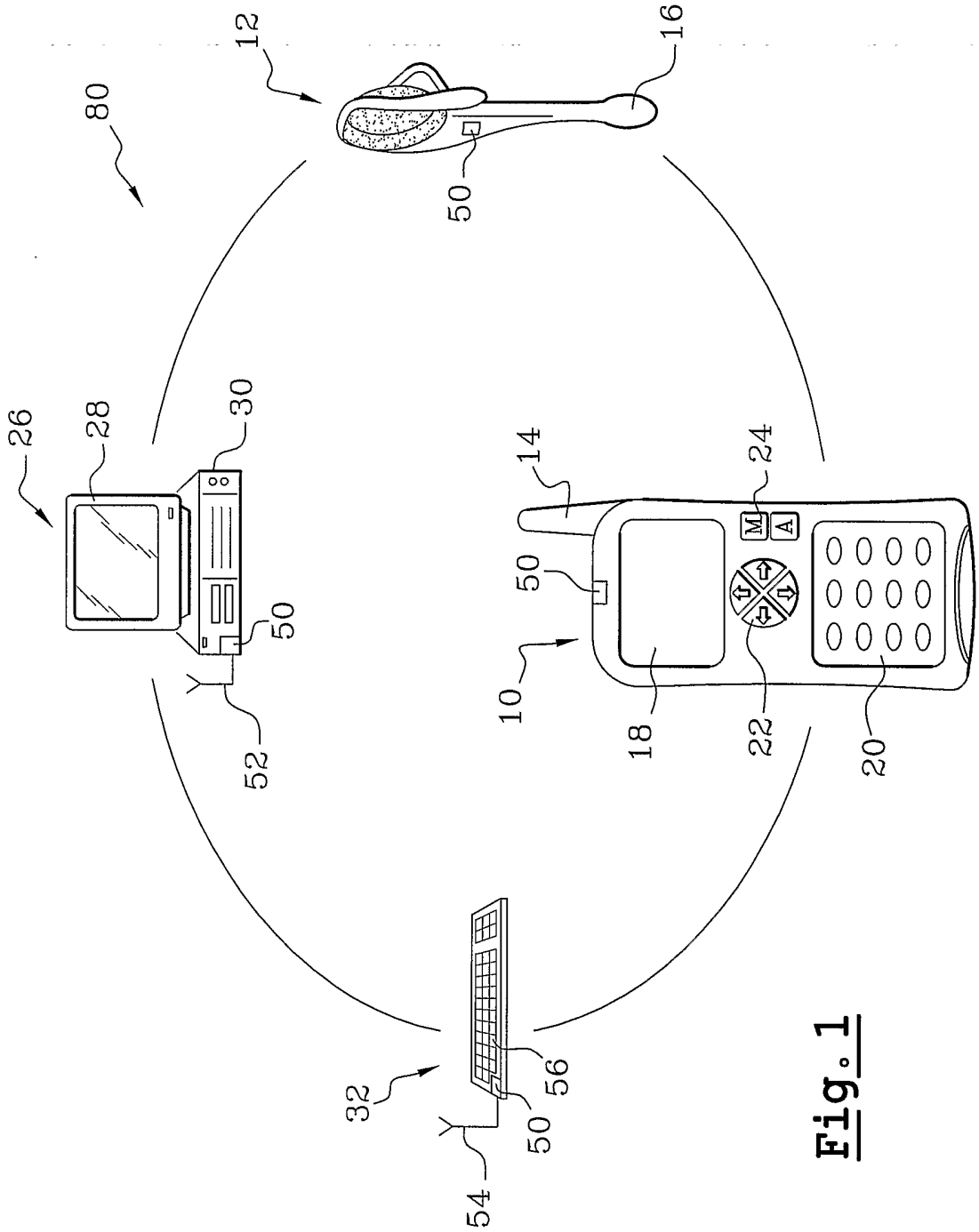


Fig.1

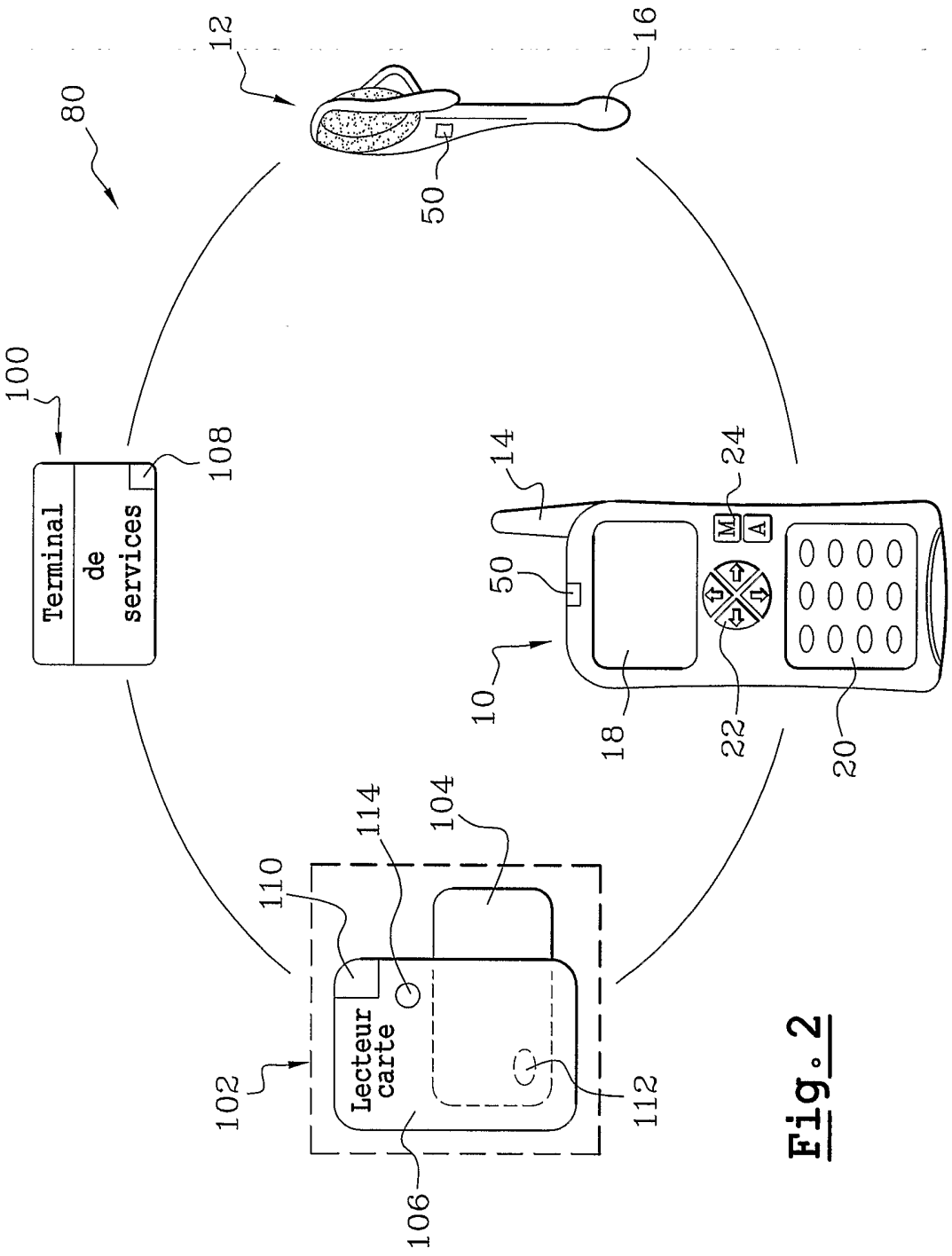

80
12
16
50
100
Terminal de services
108
14
24
M
A
50
10
18
22
20
114
104
110
Lecteur carte
102
112
106

Fig. 2