(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
24 août 2006 (24.08.2006)

PCT

(10) Numéro de publication internationale
WO 2006/087438 A1

(51) Classification internationale des brevets :
H04Q 7/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2006/000161

(22) Date de dépôt international :
24 janvier 2006 (24.01.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0501636 17 février 2005 (17.02.2005) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **DANET, Pierre-Yves** [FR/FR]; 16, route de Kernu, F-22700 Louannec (FR). **BORSIER, Céline** [FR/FR]; Lochrist, F-22450 Coatreven (FR). **PICQUENOT, David** [FR/FR]; 3, impasse du Grand Clos, F-14280 Saint Contest (FR).

(74) Mandataires : **BENTZ, Jean-Paul** etc.; Novagraaf Technologies, 122, rue Edouard Vaillant, F-92593 Levallois Perret (FR).

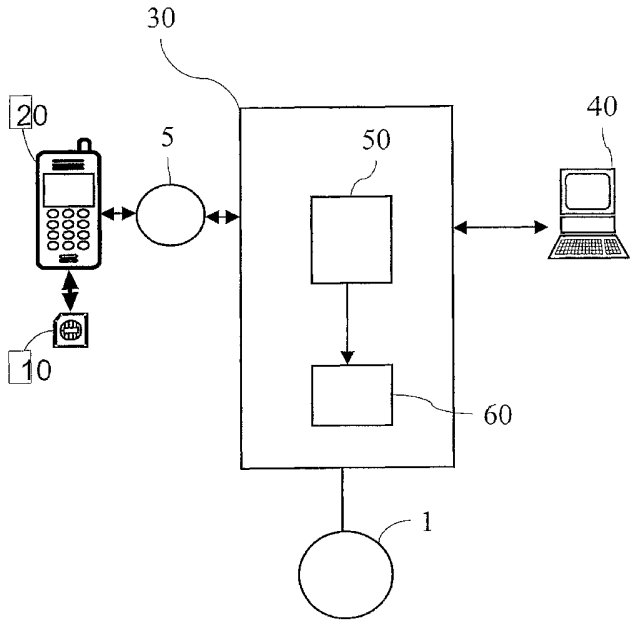
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR ACCESSING A SIM CARD HOUSED IN A MOBILE TERMINAL BY MEANS OF A DOMESTIC GATEWAY

(54) Titre : PROCEDE ET DISPOSITIF D'ACCES A UNE CARTE SIM LOGEE DANS UN TERMINAL MOBILE PAR L'INTERMEDIAIRE D'UNE PASSERELLE DOMESTIQUE



(57) Abstract: The invention relates to a method of exchanging data between an application running on a terminal (40) and a memory card (10). The inventive method comprises the following steps consisting in: transmitting data over a wireless link (5) between (i) a gateway (30) which interconnects the terminal with a telecommunication network (1) and (ii) a mobile terminal (20) which is equipped with the memory card (10), said mobile terminal being used for the transmission of data between the memory card and the wireless link.

[Suite sur la page suivante]

WO 2006/087438 A1

ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

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'échange de données entre une application s'exécutant sur un terminal (40) et une carte à mémoire (10), ledit procédé comprenant des étapes consistant à transmettre les données par une liaison sans fil (5) entre une passerelle (30) interconnectant ledit terminal avec un réseau de télécommunication (1), et un terminal mobile (20) équipé de la carte à mémoire (10), le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.

PROCEDE ET DISPOSITIF D'ACCES A UNE CARTE SIM LOGEE DANS UN TERMINAL MOBILE PAR L'INTERMEDIAIRE D'UNE PASSERELLE DOMESTIQUE

La présente invention concerne le domaine des télécommunications et en particulier les services accessibles par l'intermédiaire d'un équipement central, connecté d'une part, à un réseau de télécommunication public, tel que le réseau Internet, et, d'autre part, à un réseau local, permettant de gérer d'une manière centralisée l'ensemble des flux liés aux différents services accédés par l'utilisateur.

L'invention peut trouver une application particulièrement intéressante, parmi de nombreuses autres, dans le domaine de l'authentification d'un utilisateur, lorsque ce dernier souhaite accéder à un service par l'intermédiaire d'un terminal connecté à une passerelle, dite « passerelle domestique », permettant d'interconnecter différents terminaux de communication domestiques (PC, TV, centrale d'alarme...) avec des réseaux de télécommunication.

Une telle passerelle permet donc de supporter une pluralité de services de communication à domicile : Internet, télévision, VoIP, consoles de jeux.... Elle est typiquement dotée de fonctionnalités sans fil dites « wireless » autour de normes Ethernet, Wi-Fi et Bluetooth. Elle peut aussi disposer d'autres moyens de communication locale, comme infrarouge ou NFC (Near Field Communication, technologie sans contact). Une "passerelle domestique" a ainsi pour vocation à

s'interconnecter avec différents types d'équipements de communication dans la maison.

Actuellement, l'authentification d'un utilisateur, lorsqu'il souhaite accéder à un service porté par la passerelle domestique à partir de n'importe quel terminal de communication du domicile, est réalisée au niveau du terminal lui-même. Ce processus peut nécessiter soit une authentification basique de type identifiant et mot de passe, soit une authentification forte de type signature électronique, afin de pouvoir d'une part, protéger l'accès au service et, d'autre part, personnaliser le contenu accédé.

Pour ce qui concerne l'authentification basique, elle est typiquement réalisée par la saisie manuelle d'un identifiant et d'un mot de passe sur un clavier du terminal. Une telle authentification s'avère ainsi peu fiable et peu ergonomique.

En cas d'authentification forte demandée, l'utilisateur doit disposer d'une clé électronique par exemple de type dongle USB, ce qui implique que le terminal soit équipé d'un port USB et que la clé soit introduite dans celui-ci pour que le terminal puisse lire les données d'authentification contenues dans la clé. Cette dernière solution est peu envisageable car la majorité des terminaux de communication domestiques ne disposent pas de ports USB. Par ailleurs, cette solution n'est pas non plus ergonomique pour l'utilisateur.

Dans le domaine de l'accès d'un utilisateur à un réseau de télécommunication par l'intermédiaire d'un terminal de type PC, il est connu de mettre en œuvre

une procédure d'authentification impliquant une carte à mémoire et en particulier les cartes à mémoire SIM (Subscriber Identity Module) du terminal mobile de l'utilisateur, qui sont couramment utilisées pour l'authentification dans les réseaux mobiles de type GSM (Global System for Mobile Communication). En effet, la carte SIM du mobile permet avantageusement d'automatiser un processus d'authentification et de libérer ainsi l'utilisateur des fastidieuses saisies de codes.

Dans un tel système, chaque poste utilisateur doit alors comprendre un terminal de type PC équipé de moyens de lecture d'une carte SIM, en vue de pouvoir utiliser les informations mémorisées par une carte SIM pour les transmettre vers un serveur d'authentification couplé au réseau de télécommunication.

Or, la majorité des terminaux de communication qui sont interconnectés avec des réseaux de télécommunication par l'intermédiaire d'une passerelle domestique, ne disposent pas de lecteur de carte SIM.

Dans ce contexte, il est difficilement envisageable de prévoir un accès à une carte SIM pour les différents équipements domestiques connectés à la passerelle, en vue par exemple de mettre en œuvre un processus d'authentification, sans avoir préalablement équipé chacun d'eux d'un lecteur de carte SIM et introduit une carte SIM dans celui-ci. L'ergonomie d'un tel système s'en trouverait fortement réduite.

La présente invention a pour but de remédier à ces inconvénients. Cet objectif est atteint par la prévision d'un procédé d'échange de données entre un

terminal et une carte à mémoire accessible au terminal, par l'intermédiaire d'une passerelle domestique à laquelle le terminal est relié.

Avec cet objectif en vue, l'invention a pour objet un procédé d'échange de données entre une application s'exécutant sur un terminal et une carte à mémoire, ledit procédé comprenant des étapes consistant à transmettre les données par une liaison sans fil entre une passerelle interconnectant ledit terminal avec un réseau de télécommunication, et un terminal mobile équipé de la carte à mémoire, le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.

De préférence, les données échangées entre le terminal et la carte à mémoire par l'intermédiaire de la passerelle permettent la mise en œuvre de fonctions de sécurité offertes par ladite carte à mémoire et sont utilisées pour sécuriser des applications à partir dudit terminal.

Selon un mode de réalisation, la liaison sans fil est une liaison conforme au protocole Bluetooth, une liaison de type infrarouge ou une liaison de type NFC.

L'invention concerne également un dispositif d'échange de données entre une application s'exécutant sur un terminal et une carte à mémoire, caractérisé en ce qu'il comprend des moyens d'établissement d'une liaison sans fil entre une passerelle interconnectant ledit terminal avec un réseau de télécommunication, et un terminal mobile équipé de la carte à mémoire, et des moyens pour échanger des données par la liaison sans fil entre la passerelle et la carte mémoire insérée

dans le terminal mobile, le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.

De préférence, les données échangées entre le terminal et la carte à mémoire par l'intermédiaire de la passerelle sont des données permettant la mise en œuvre de fonctions de sécurité offertes par ladite carte à mémoire et sont utilisées pour sécuriser des applications à partir dudit terminal.

De préférence, la liaison sans fil est une liaison conforme au protocole Bluetooth, une liaison de type infrarouge ou une liaison de type NFC.

Selon un mode de réalisation, le dispositif comprend un module client installé dans la passerelle et un module serveur installé dans le terminal mobile, conçus pour établir des communications par l'intermédiaire de la liaison sans fil entre la passerelle à laquelle est relié le terminal et la carte à mémoire insérée dans le terminal mobile.

De préférence, le module client et le module serveur sont conformes aux spécifications SIM Access Profile.

Avantageusement, le module serveur installé dans le terminal mobile comprend des moyens de conversion de commandes APDU reçues à destination de la carte à mémoire.

Avantageusement, le dispositif comprend, installés dans le terminal, un module implémentant un protocole d'accès aux cartes à mémoire, associé à un module d'interface avec un module d'accès installé dans la passerelle, prévu pour accéder à la carte à mémoire

insérée dans le terminal mobile par l'intermédiaire de la liaison sans fil.

Selon un mode de réalisation, le module d'interface installé dans le terminal est conforme aux spécifications du standard PC/SC et est conçu pour permettre de dialoguer avec tout type de lecteur de carte à mémoire par l'intermédiaire d'un pilote d'adaptation, ledit module d'accès installé dans la passerelle faisant office de pilote d'adaptation.

Selon un autre mode de réalisation, le module d'interface installé dans la passerelle implémente une interface directe avec la passerelle.

Avantageusement, le module d'accès, installé dans la passerelle, est conçu pour recevoir du module d'interface, installé dans le terminal, des messages de transmission de commandes à appliquer à la carte à mémoire insérée dans le terminal mobile, et pour accéder à un module client installé dans la passerelle, qui est conçu pour établir des communications par l'intermédiaire de la liaison sans fil avec un module serveur installé dans le terminal mobile et ayant accès à la carte à mémoire insérée dans le terminal mobile, pour transmettre lesdits messages à la carte à mémoire.

De préférence, les messages échangés entre le module d'interface installé dans le terminal et le module d'accès installé dans la passerelle à laquelle est relié ledit terminal, sont conformes au protocole SOAP.

L'invention concerne encore une passerelle domestique interconnectant au moins un terminal avec au moins un réseau de télécommunication, caractérisé en ce

que ladite passerelle comprend des moyens d'établissement d'une liaison sans fil avec un terminal mobile équipé d'une carte à mémoire, et des moyens pour échanger des données par la liaison sans fil avec la carte mémoire insérée dans le terminal mobile.

L'architecture mise en place par l'invention telle qu'elle vient d'être décrite permet donc avantageusement de fournir à des applications localisées sur des terminaux utilisateurs connectés à une passerelle domestique, un service porté par la passerelle permettant l'accès à une carte à mémoire localisée dans un terminal mobile via une liaison locale sans fil.

L'implémentation générique associée à ce fonctionnement met avantageusement en œuvre une application localisée sur la carte à mémoire offrant des fonctions de sécurité au service porté par la passerelle domestique, qui est accessible depuis un terminal connecté à cette passerelle.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture d'un mode de réalisation préféré de l'invention, donné à titre d'exemple illustratif et non limitatif, avec référence aux figures annexées dans lesquelles :

-la figure 1 représente un schéma fonctionnel d'un système d'échange de données entre une carte à mémoire logée dans un terminal mobile et un terminal utilisateur par l'intermédiaire de la passerelle à laquelle est relié le terminal utilisateur, et

-la figure 2 illustre les différentes couches logicielles mises en œuvre dans les différentes entités selon l'invention.

La figure 1 représente les échanges mis en œuvre selon l'invention, pour l'accès à une carte à mémoire 10 localisée dans un terminal mobile 20 par un terminal 40, lorsqu'un utilisateur souhaite accéder, par l'intermédiaire du terminal, à un service porté par une passerelle domestique 30 à laquelle est relié le terminal 40. L'accès à la carte à mémoire dans ce contexte peut par exemple être mis en œuvre en vue d'accéder à des fonctions de sécurité offertes par la carte à mémoire, permettant de sécuriser des applications à partir du terminal 40.

La carte à mémoire peut être une carte SIM, une carte USIM ou toute autre carte à mémoire standardisée UICC (« UMTS Integrated Circuit Card », soit carte de circuit intégré pour UMTS), implantée dans un terminal mobile raccordé à un réseau de type UMTS («Universal Mobile Telecommunication System »), telle que définie par les standards du Groupe de normalisation 3GPP (« Third Generation partnership Project ») et de l'ETSI (« European Telecommunications Standards Institute »).

Le terminal 40 permet donc l'exécution d'applications et fournit une connexion à un réseau IP 1 (Internet Protocol) via la passerelle 30. Il peut s'agir de n'importe quel terminal de communication du domicile (téléviseur, PC, PDA, portable...).

Un module d'accès 60 est pour ce faire intégré à la passerelle domestique 30, laquelle doit par ailleurs

disposer d'une liaison locale sans fil de type Bluetooth, infrarouge, NFC ou autre.

Ainsi, lorsque l'utilisateur souhaite accéder à un service porté par la passerelle domestique 30 à partir du terminal 40, il se connecte tout d'abord sur le portail d'accès aux services 50 porté par la passerelle en utilisant un identifiant, par exemple son nom ou un pseudo. Le module d'accès 60 de la passerelle 30 est alors prévu pour établir une connexion avec la carte SIM 10 insérée dans le terminal mobile 20 correspondant par l'intermédiaire de la liaison sans fil 5, par exemple de type Bluetooth.

Ce processus d'accès à une carte SIM par exemple via la passerelle domestique et la liaison sans fil peut avantageusement être utilisée pour authentifier l'utilisateur, lorsque ce dernier souhaite accéder à un service porté par la passerelle à partir du terminal 40. De cette manière, l'utilisateur n'a pas besoin de disposer d'une carte SIM spécifique pour s'authentifier et accéder au service souhaité ou de manipuler la carte SIM de son terminal mobile pour l'insérer dans un autre lecteur connecté à son terminal de communication.

En effet, une fois que la liaison entre la passerelle 30 et la carte SIM est effectuée par l'intermédiaire du module d'accès 60 et de la liaison sans fil 5, le module d'accès peut récupérer les informations d'authentification codées sur la carte SIM et ainsi vérifier les droits correspondants. Si les droits permettent à l'utilisateur d'accéder au service demandé, la passerelle transmet l'identifiant et le mot de passe correspondant vers le terminal connecté sur le

réseau local domestique. Dans le cas contraire, si les droits ne permettent pas à l'utilisateur d'accéder au service, un message de refus lui est notifié.

Selon cet exemple d'application où l'accès à une carte SIM distante par l'intermédiaire de la passerelle est dédié à l'authentification de l'utilisateur, le module d'accès 60 se présente donc sous la forme d'une fonction logicielle mise à disposition des différents services et applications portés par la passerelle domestique. Ainsi, lorsque le portail d'accès aux services ou un terminal connecté au réseau local domestique émet une requête pour authentifier l'utilisateur lorsque ce dernier souhaite accéder à un service porté par la passerelle, le module d'accès intégré à la passerelle détermine l'adresse du terminal mobile en fonction de l'identifiant de l'utilisateur et transmet une demande d'authentification vers la carte SIM du mobile en utilisant la liaison sans fil. Le module d'accès embarqué sur la passerelle permet donc de relayer les demandes d'authentification du portail d'accès aux services ou des différents terminaux connectés au réseau local domestique vers la carte SIM insérée dans le terminal mobile.

Sur ce terminal mobile, il est prévu des moyens d'accès à la carte SIM, offrant ainsi une interface de communication avec la carte SIM, pour router les demandes d'authentification reçues du module d'accès intégré à la passerelle vers une application localisée dans la carte SIM. Toujours dans le cadre de l'exemple où l'accès à la carte SIM est dédié à l'authentification, il s'agit d'une application

d'authentification permettant d'authentifier l'utilisateur par demande de code PIN et éventuellement calcul cryptographique d'un certificat d'authentification. Des données d'authentification statiques (mots de passe) peuvent aussi être stockées dans la carte SIM et envoyées chiffrées à la passerelle. A la réception de la réponse, le module d'accès intégré à la passerelle authentifie l'utilisateur à partir de son identifiant et des données d'authentification reçues et effectue une vérification des droits d'accès au service souhaité en fonction de l'authentification.

Sur le plan logiciel, le terminal mobile 20 et la passerelle domestique 30 mettent en œuvre un ensemble de protocoles et de procédures appelées SAP (SIM Access Profile) conçues dans le cadre du protocole Bluetooth pour donner un accès à une carte SIM insérée dans un terminal par l'intermédiaire d'une liaison Bluetooth 5, d'une manière totalement transparente.

Ainsi, sur la figure 2, le terminal mobile 20 comprend un module serveur SAP 21 qui échange des messages d'un côté avec la carte SIM 10 par l'intermédiaire d'un lecteur 22 conforme à la norme ISO 7816-3, et de l'autre avec la liaison Bluetooth par l'intermédiaire d'une couche 23 implémentant le protocole RFCOMM (Serial Cable Emulation Protocol) émulant une liaison série, et une couche de bas niveau 24 permettant d'établir une liaison radio Bluetooth 5 avec d'autres terminaux, en l'occurrence avec la passerelle domestique 30.

La carte SIM comprend préférentiellement une application 25 de type applet Java, prévue pour fournir des services de sécurité, tels que signature, authentification PKI (Public Key Infrastructure), authentification SKI (Secret Key Infrastructure) ou de type coffre-fort de mots de passe (liste de services non limitative).

Selon l'invention, la passerelle domestique 30 comprend un module client SAP 31, qui communique avec le module serveur SAP 21 par exemple par l'intermédiaire d'une couche 32 implémentant le protocole RFCOMM et une couche de bas niveau 33 d'établissement de liaison radio Bluetooth 5, ces trois couches étant rassemblées dans un module Bluetooth 34.

Les modules SAP serveur 21 et client 31 permettent donc d'échanger des messages avec la carte SIM, et de lui appliquer des commandes, comme des commandes de mise sous/hors tension de la carte SIM.

Le module SAP client 31 est ainsi conçu pour exécuter une procédure de connexion avec le module SAP serveur 21 par l'intermédiaire de la liaison Bluetooth, et une procédure de déconnexion. Lorsqu'une liaison est établie, le module SAP serveur 21 est conçu pour interroger le lecteur 22 de carte SIM et la carte SIM 10 susceptible d'être lue par le lecteur, et renvoyer au module SAP client des informations sur l'état du lecteur 22, sur la présence d'une carte SIM dans le lecteur et sur l'état de la carte SIM.

Le module SAP client 31 est en particulier conçu pour émettre des ordres destinés à la carte SIM de mise sous/hors tension, d'initialisation, et de commande

contenant des messages APDU (Application Protocol Data Units), le module SAP serveur étant conçu pour relayer ces commandes pour les appliquer à la carte SIM via le lecteur 22. Le module SAP serveur est également conçu pour avertir le module SAP client de tous les événements de changement d'état de la carte SIM insérée dans le lecteur, par exemple à la suite d'une action de l'utilisateur d'insertion ou de retrait de la carte du lecteur.

Par ailleurs, la procédure d'accès à la carte SIM qui est implémentée côté terminal 40 est effectué à l'aide d'un module client 44, installé dans le terminal 40, et ayant accès à un module d'interface PC/SC (Personal Computer / Smart Card) 45 avec une carte SIM. Ce module 44 peut demander un accès à la carte SIM par exemple pour des besoins d'authentification. Il peut alors s'agir d'un logiciel de gestion d'identités sur PC (ex: client VPN, navigateur WEB utilisant SSL v3), téléviseur,... ou un « plug-in » associé à un navigateur Web ayant besoin de lire des données d'authentification dans une carte SIM distante.

Le module 44 fait donc appel à des fonctions d'accès et de commande de la carte SIM, réalisées par le module d'interface PC/SC 45. Le module d'interface PC/SC 45 est habituellement conçu pour s'interfacer avec des lecteurs de cartes à puce (carte à mémoire ou à microprocesseur) ou cartes SIM par l'intermédiaire de pilotes adaptés au type de lecteurs, permettant ainsi à des applications de dialoguer avec ces lecteurs. L'invention met alors en œuvre un module d'accès 35, faisant office de pilote, implémenté au niveau de la

passerelle domestique 30, conçu pour relayer et adapter les messages échangés entre le module d'interface 45 implémenté côté terminal et le module client SAP 31 implémenté côté passerelle, ces messages contenant des informations échangées avec la carte SIM 10.

Pour communiquer avec le module d'accès 35, le module d'interface 45 comprend un module de gestion de ressources 47 et un module fournisseur de services 46. Le module de gestion de ressources 47 est conçu pour spécifier les terminaux mobiles utilisables par le système, spécifier le terminal mobile actif, c'est-à-dire celui qui sera utilisé par le système en cas de requête sur le module d'interface 45, et rendre ces informations disponibles à plusieurs applications telles que l'application d'authentification 44. Ce module est également conçu pour gérer les demandes d'accès aux cartes à puces émises par les applications, et commander les cartes à puce.

Le module fournisseur de services 46 est conçu pour offrir aux applications des fonctions enchaînant plusieurs commandes appliquées à une carte à puce pour réaliser une seule fonction d'accès ou de traitement des informations fournies par celle-ci, ces fonctions incluant notamment des fonctions cryptographiques et d'authentification.

Pour router les messages de commandes APDU vers le terminal mobile, le processus de routage des APDU utilise donc les services offerts par module d'accès 35 sur la passerelle. Le module d'accès 35 est conçu pour recevoir du module d'interface 45 des messages de transmission de commandes à appliquer à la carte SIM,

ces messages provenant de l'application cliente 44, pour transmettre ces messages au module SAP client 31 pour que les commandes qu'ils contiennent soient finalement transmises à la carte à puce 10. Il est également conçu pour recevoir les réponses de la carte SIM et pour retransmettre ces réponses à l'application 44.

L'accès à la carte SIM 10 distante localisée dans le terminal mobile 20 peut ainsi être effectué à l'aide du module d'accès 35 sur la passerelle, qui permet une gestion des flux en mode proxy correspondant aux différentes demandes d'accès aux cartes à puces émises par les applications prévues pour s'exécuter sur les différents terminaux connectés au réseau local domestique.

Par exemple, le module d'accès 35 côté passerelle propose une interface de type SOAP. Le protocole SOAP est un protocole de communication s'appuyant sur le XML et le HTTP, qui permet d'assurer l'interopérabilité des applications. On accède ainsi à la passerelle en IP, laquelle se charge alors, par l'intermédiaire du module d'accès et du module Bluetooth, d'envoyer à destination de la carte SIM les messages contenant des commandes APDU émises par les applications. L'interface SOAP permet donc la communication avec une carte SIM par APDU. Les fonctions appelées au niveau de cette interface doivent provoquer l'exécution d'une même fonction au niveau du module SAP client 31 localisé dans la passerelle.

Il convient de noter que le mode de réalisation décrit plus haut basé sur l'implémentation du module

d'interface PC/SC côté terminal 40, est plus particulièrement judicieuse dans les cas où l'application cliente utilise habituellement PC/SC (c'est le cas des logiciels de cryptographie de type CSP ou PKCS#11 utilisés par les clients VPN, les navigateurs WEB, les logiciels de messagerie, etc...). De cette façon, le procédé selon l'invention s'intègre sans impacts aux architectures existantes. Dans d'autre cas où l'application n'utilise pas PC/SC, il peut être plus pertinent d'utiliser en tant que variante une interface directe de type SOAP ou TCP vers la passerelle, ce qui permet avantageusement d'accélérer les échanges en supprimant le processus effectué par l'interface PC/SC.

Selon l'invention, un autre mode de réalisation est prévu, visant à proposer une alternative à l'implémentation du module SAP serveur sur le terminal mobile. En effet, lorsqu'on utilise le protocole SAP en mode serveur sur le terminal mobile, ce dernier est complètement transparent pour l'utilisateur et se comporte finalement comme un simple lecteur de carte. On est alors dépendant de l'implémentation choisie par le constructeur de mobile, ce qui empêche d'avoir une maîtrise sur l'accès à certaines données dans la carte SIM.

Selon ce mode de réalisation, le terminal mobile comprend un module de conversion de commandes à destination de la carte SIM, différent d'un serveur SAP. Un exemple d'utilisation serait de permettre la saisie du code PIN sur le terminal mobile lui-même. Ainsi, dans le cadre d'un processus d'authentification

de l'utilisateur impliquant un accès à la carte SIM selon l'invention, plutôt que de demander le code PIN sur le terminal utilisateur, celui-ci serait demandé sur le terminal mobile. De cette manière, le code PIN n'aurait pas à transiter sur le lien IP entre la passerelle et le terminal utilisateur, ce qui est préférable en terme de sécurité.

Pour ce faire, le module de conversion du terminal mobile se présente sous la forme d'un serveur qui reçoit des commandes APDU, les interprète et les transforme en appel de fonctions de type API RIL (« Radio Interface Layer ») par exemple dans le cas d'une implémentation sur plate-forme mobile Microsoft Windows Mobile. Le module d'interprétation s'appuie alors dans l'exemple de réalisation sur une bibliothèque de fonctions créée par Microsoft, permettant de dialoguer directement avec un modem et notamment avec la carte SIM au travers de diverses fonctions.

De cette manière, le module de conversion implémenté sur le terminal mobile va permettre d'accéder à certaines données de la carte SIM tel que la taille de certains enregistrements, ainsi que les informations qu'ils contiennent.

Plus précisément, le module de conversion du terminal mobile coopère avec une application d'interface réseau. Cette application a pour rôle d'établir une connexion sans fil, de type Bluetooth ou autre, avec un client lors d'une requête d'accès reçue de la part de ce dernier. Les spécifications de cette interface pourront être avantageusement conformes aux

spécifications du protocole SAP. Une fois cette connexion établie, l'interface réseau a pour but de diriger les informations vers le module d'interprétation, si celui-ci est demandé par le client.

Le module de conversion, basé par exemple sur l'API RIL de Microsoft, va alors permettre d'envoyer la requête SIM et d'en lire sa réponse. Toutefois, étant basé sur l'API RIL, il doit d'abord faire la conversion des requêtes APDU. Pour cela, il aura pour charge dans un premier temps de transformer la requête APDU en la commande SIM qui lui correspond. Si aucune commande ne correspond, un message d'erreur sera directement renvoyé au client. Une fois la commande exécutée avec les bons paramètres, la carte SIM renvoie une réponse que le module de conversion aura pour charge de mettre au format de l'APDU pour la renvoyer vers le client.

Si la description qui précède décrit plus particulièrement une application de l'invention dans un contexte d'authentification d'un utilisateur lorsqu'il souhaite accéder à un service porté par une passerelle domestique à partir d'un terminal connecté à celle-ci, il va de soi que l'accès à une carte SIM distante via une liaison sans fil par l'intermédiaire d'une passerelle domestique peut être utilisé dans de nombreuses autres applications, telles que par exemple des applications de signature, de chiffrement, de stockage de données numériques, etc. Dans le cas d'une application de signature, de chiffrement ou de déchiffrement, un certificat associé à une clé secrète correspondants à l'utilisateur pourront être stockés

dans la carte SIM et utilisés par un logiciel (« middleware ») de type PKCS#11 localisé soit dans la passerelle, soit dans le terminal. D'une manière plus générale, l'invention peut être utilisée pour échanger des données avec une carte à mémoire par l'intermédiaire d'une passerelle domestique. L'implémentation générique associée à ce fonctionnement met en œuvre une application localisée sur la carte SIM offrant des fonctions de sécurité (ex:applet de signature, déchiffrement, de stockage sécurisé, de comptage/décomptage sécurisé, etc...) à un service porté par une passerelle domestique et accessible depuis un terminal connecté à cette passerelle.

REVENDICATIONS

1. Procédé d'échange de données entre une application s'exécutant sur un terminal (40) et une carte à mémoire (10), ledit procédé comprenant des étapes consistant à transmettre les données par une liaison sans fil (5) entre une passerelle (30) interconnectant ledit terminal avec un réseau de télécommunication (1), et un terminal mobile (20) équipé de la carte à mémoire (10), le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.

2. Procédé selon la revendication 1, caractérisé en ce que les données échangées entre le terminal (40) et la carte à mémoire (10) par l'intermédiaire de la passerelle (30) permettent la mise en œuvre de fonctions de sécurité offertes par ladite carte à mémoire (10) et sont utilisées pour sécuriser des applications à partir dudit terminal (40).

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que la liaison sans fil (5) est une liaison conforme au protocole Bluetooth, une liaison de type infrarouge ou une liaison de type NFC.

4. Dispositif d'échange de données entre une application s'exécutant sur un terminal (40) et une carte à mémoire (10), caractérisé en ce qu'il comprend des moyens (34, 21, 23, 24) d'établissement d'une

liaison sans fil (5) entre une passerelle (30) interconnectant ledit terminal avec un réseau de télécommunication (1), et un terminal mobile (20) équipé de la carte à mémoire (10), et des moyens pour échanger des données par la liaison sans fil entre la passerelle (30) et la carte mémoire insérée dans le terminal mobile, le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.

5. Dispositif selon la revendication 4, caractérisé en ce que les données échangées entre le terminal (40) et la carte à mémoire (10) par l'intermédiaire de la passerelle (30) sont des données permettant la mise en œuvre de fonctions de sécurité offertes par ladite carte à mémoire (10) et sont utilisées pour sécuriser des applications à partir dudit terminal (40).

6. Dispositif selon la revendication 4 ou 5, caractérisé en ce que la liaison sans fil (5) est une liaison conforme au protocole Bluetooth, une liaison de type infrarouge ou une liaison de type NFC.

7. Dispositif selon l'une quelconque des revendications 4 à 6, caractérisé en ce qu'il comprend un module client (31) installé dans la passerelle (30) et un module serveur (21) installé dans le terminal mobile (20), conçus pour établir des communications par l'intermédiaire de la liaison sans fil entre la passerelle (30) à laquelle est relié le terminal (40)

et la carte à mémoire (10) insérée dans le terminal mobile.

8. Dispositif selon la revendication 7, caractérisé en ce que le module client (31) et le module serveur (21) sont conformes aux spécifications SIM Access Profile.

9. Dispositif selon la revendication 7 ou 8, caractérisé en ce que le module serveur installé dans le terminal mobile comprend des moyens de conversion de commandes APDU reçues à destination de la carte à mémoire.

10. Dispositif selon l'une quelconque des revendications 4 à 9, caractérisé en ce qu'il comprend, installés dans le terminal (40), un module (44) implémentant un protocole d'accès aux cartes à mémoire, associé à un module d'interface (45) avec un module d'accès (35) installé dans la passerelle (30), prévu pour accéder à la carte à mémoire insérée dans le terminal mobile par l'intermédiaire de la liaison sans fil (5).

11. Dispositif selon la revendication 10, caractérisé en ce que le module d'interface (45) installé dans le terminal (40) est conforme aux spécifications du standard PC/SC et est conçu pour permettre de dialoguer avec tout type de lecteur de carte à mémoire par l'intermédiaire d'un pilote d'adaptation, ledit module d'accès (35) installé dans

la passerelle (30) faisant office de pilote d'adaptation.

12. Dispositif selon la revendication 10, caractérisé en ce que le module d'interface installé dans la passerelle implémente une interface directe avec la passerelle.

13. Dispositif selon l'une quelconque des revendications 10 à 12, caractérisé en ce que le module d'accès (35), installé dans la passerelle, est conçu pour recevoir du module d'interface (45), installé dans le terminal (40), des messages de transmission de commandes à appliquer à la carte à mémoire (10) insérée dans le terminal mobile (20), et pour accéder à un module client (31) installé dans la passerelle, qui est conçu pour établir des communications par l'intermédiaire de la liaison sans fil (5) avec un module serveur (21) installé dans le terminal mobile et ayant accès à la carte à mémoire insérée dans le terminal mobile, pour transmettre lesdits messages à la carte à mémoire (10).

14. Dispositif selon la revendication 13, caractérisé en ce que les messages échangés entre le module d'interface (45) installé dans le terminal (40) et le module d'accès (35) installé dans la passerelle (30) à laquelle est relié ledit terminal, sont conformes au protocole SOAP.

15. Passerelle domestique interconnectant au moins un terminal (40) avec au moins un réseau de télécommunication (1), caractérisé en ce que ladite passerelle (30) comprend des moyens (34) d'établissement d'une liaison sans fil (5) avec un terminal mobile (20) équipé d'une carte à mémoire (10), et des moyens (35, 31) pour échanger des données par la liaison sans fil entre une application s'exécutant sur le terminal et la carte mémoire insérée dans le terminal mobile.

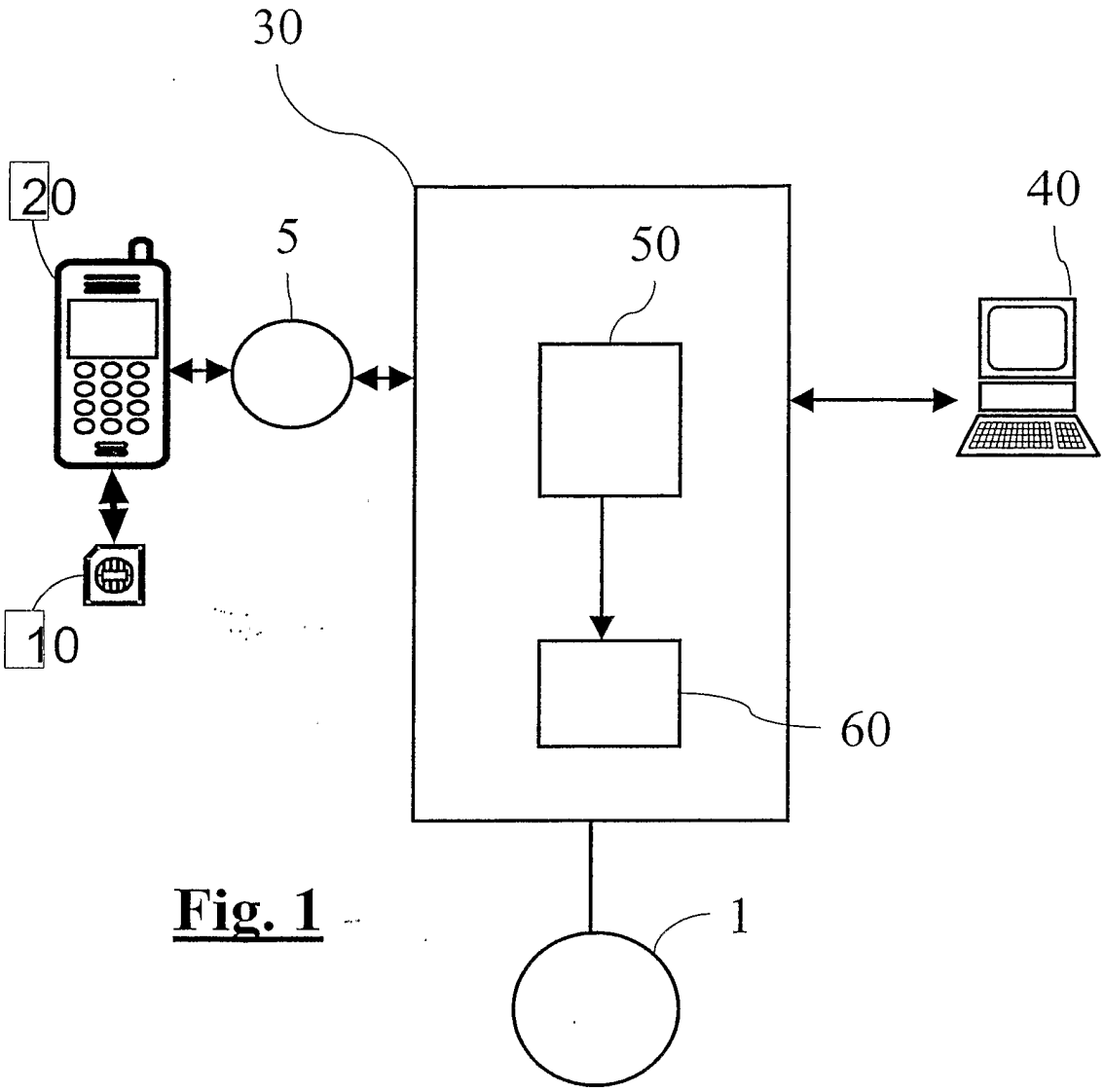


Fig. 1

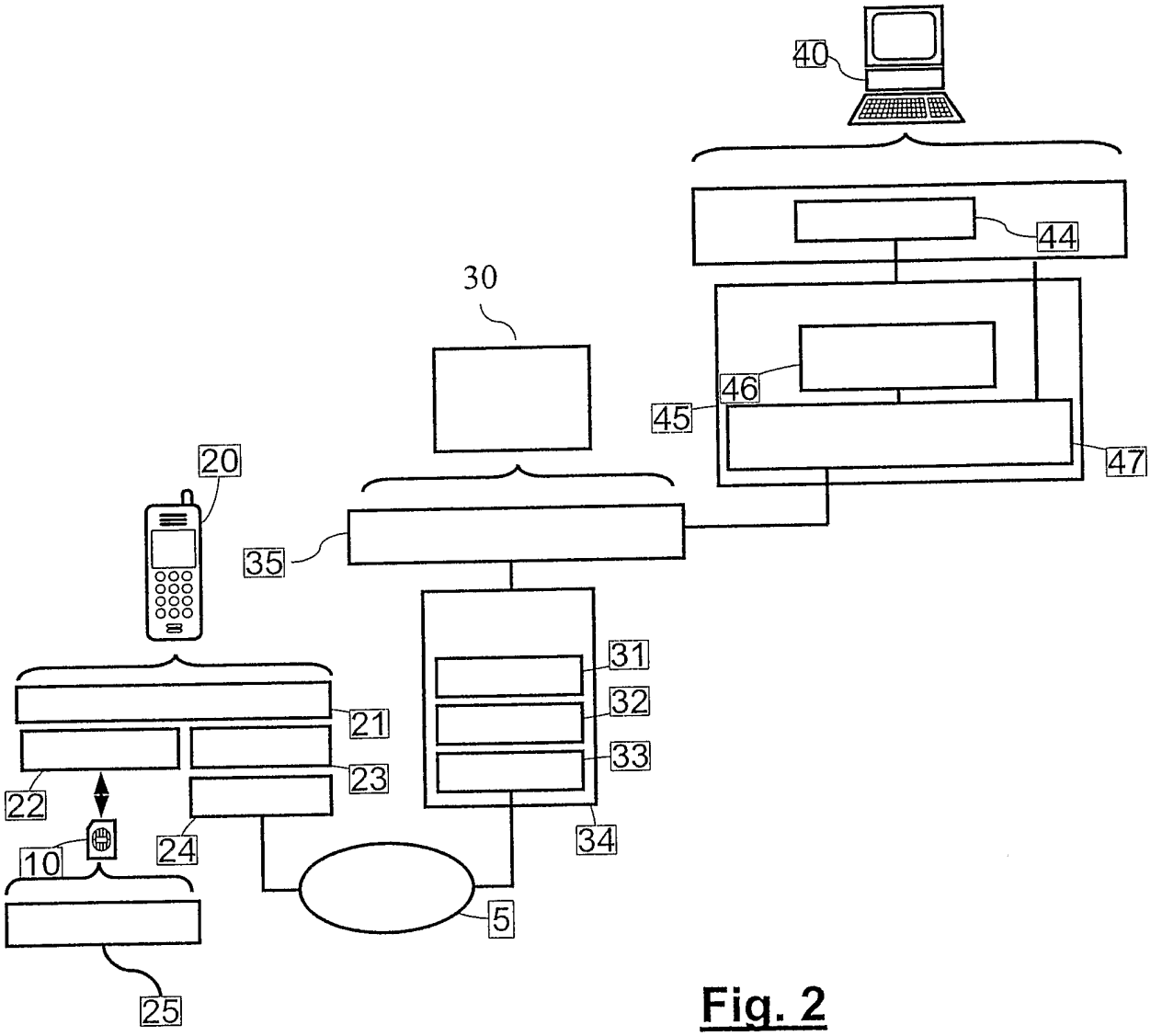


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/000161

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/030950 A1 (CHEN STEVEN CHIEN-YOUNG ET AL) 18 October 2001 (2001-10-18) paragraph [0016] - paragraph [0020] figures 3-5	1,4,15
A	EP 1 130 875 A (SONY CORPORATION) 5 September 2001 (2001-09-05) paragraphs [0066] - [0072]	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 May 2006	02/06/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dionisi, M

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2006/000161

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001030950 A1	18-10-2001	NONE	
EP 1130875 A	05-09-2001	US 2006013239 A1	19-01-2006
		US 2001020241 A1	06-09-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/000161

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04Q7/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2001/030950 A1 (CHEN STEVEN CHIEN-YOUNG ET AL) 18 octobre 2001 (2001-10-18) alinéa [0016] - alinéa [0020] figures 3-5	1,4,15
A	EP 1 130 875 A (SONY CORPORATION) 5 septembre 2001 (2001-09-05) alinéas [0066] - [0072]	1-15

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
26 mai 2006	02/06/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dionisi, M

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2006/000161

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2001030950 A1	18-10-2001	AUCUN	
EP 1130875 A	05-09-2001	US 2006013239 A1	19-01-2006
		US 2001020241 A1	06-09-2001