



(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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet 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.

PROCEDE ET DISPOSITIF D'ECHANGE DE DONNEES ENTRE UN
TERMINAL CONNEXE A UN RESEAU ET UNE CARTE SIM LOGEE
DANS UN TERMINAL MOBILE.

5

La présente invention concerne le domaine des télécommunications et en particulier les services accessibles aux terminaux susceptibles de se connecter à un réseau sans fil tel que Wi-Fi basé sur la norme IEEE 802.11b.

- 10 Actuellement, l'authentification d'un utilisateur sur un réseau Wi-Fi public à l'aide d'un terminal muni d'une interface Wi-Fi, par exemple de la forme d'une carte PCMCIA (Personal Computer Memory Card International Association), est réalisée par la saisie d'un identifiant et d'un mot de passe. Une telle authentification s'avère peu fiable et peu ergonomique.

15

Pour remédier à ces inconvénients, on a prévu de mettre en œuvre une procédure d'authentification impliquant une carte à mémoire et en particulier les cartes à mémoires SIM (Subscriber Identity Module) couramment utilisées pour l'authentification dans les réseaux mobiles de type GSM (Global System
20 for Mobile Communications).

- La figure 1 montre l'architecture d'un système permettant une telle authentification et couramment utilisé par les opérateurs de réseau Wi-Fi. Dans ce système, chaque terminal d'utilisateur connecté au réseau Wi-Fi met en
25 œuvre le protocole d'authentification EAP-SIM (Extensible Authentication Protocol - Subscriber Identity Module) conçu pour authentifier l'utilisateur à l'aide d'une carte SIM utilisée pour accéder à un réseau GSM. A cet effet, ce module encapsule les messages d'authentification GSM dans des messages IP.

- 30 Dans un tel système, chaque poste utilisateur 6 comprend un terminal 1 équipé de moyens 4 pour accéder à un réseau Wi-Fi 7 et des moyens de lecture d'une carte SIM 3. Il existe ainsi des cartes modem PCMCIA permettant l'accès à un réseau Wi-Fi, munies d'un module de communication avec un réseau mobile tel que GPRS (General Packet Radio Service) et d'une carte à mémoire telle
35 qu'une carte SIM.

Dans une autre solution, le terminal 1 peut être connecté à un lecteur de carte SIM, par exemple par l'intermédiaire d'une connexion de type USB (Universal Serial Bus), l'utilisateur devant alors disposer d'une carte SIM dédiée à

l'authentification sur un réseau Wi-Fi. Ce lecteur de carte SIM peut également être intégré au module de communication Wi-Fi.

Sur le plan logiciel (figure 2), le terminal 1 est équipé d'un module 35 implémentant le protocole EAP-SIM 24 et réalisant la fonction d'authentification, d'un module de communication Wi-Fi 26 mettant en œuvre un protocole 802.11x, et d'un module d'interface PC/SC (Personal Computer / Smart Card) 25 conçu pour le système d'exploitation Windows™ de Microsoft, et permettant à des applications telles que le module EAP-SIM de dialoguer avec tous les lecteurs 39 de cartes à mémoire 3 actuellement disponibles sur le marché. A cet effet, le module d'interface 25 est associé à des pilotes 38 spécifiquement adaptés aux lecteurs de carte à mémoire connectés au terminal.

Normalement un utilisateur d'un réseau mobile 12 est authentifié dans ce réseau en fournissant au réseau mobile durant une procédure d'authentification, des informations d'authentification provenant d'une carte SIM à la suite de la saisie d'un code PIN. Ces informations sont transmises à un centre de commutation local MSC/VLR (Mobile Switching Center/Visitor Location Register) 13 du réseau mobile regroupant des données de localisation du terminal mobile. Les informations d'authentification sont ensuite transmises par l'intermédiaire d'un réseau spécialisé SS7 14 à un registre local HLR (Home Location Register) 15 où est enregistré l'utilisateur et regroupant les informations nécessaires à l'authentification de l'utilisateur. L'ensemble des informations fournies par le registre local HLR et par le terminal de l'utilisateur sont traitées par un serveur d'authentification 16 qui fournit en réponse le résultat de l'authentification de l'utilisateur.

Dans le cas d'un réseau Wi-Fi, on a prévu d'utiliser les informations d'authentification mémorisées par une carte SIM et de les transmettre par l'intermédiaire du réseau Wi-Fi, d'un point d'accès 9 permettant d'accéder à un réseau IP (Internet Protocol) 10, à un serveur d'authentification 11 couplé au réseau IP. Ce serveur d'authentification 11 par exemple de type serveur RADIUS (Remote Authentication Dial In User Service) est conçu pour accéder au serveur d'authentification 16 du réseau mobile, pour authentifier l'utilisateur sur la base des informations d'authentification contenues dans la carte SIM de celui-ci. A cet effet, le serveur d'authentification 11 est connecté au réseau 14 par l'intermédiaire d'une passerelle MAP (Mobile Application Part) 17, et accède ainsi au serveur d'authentification 16 du réseau mobile.

Si l'utilisateur possède un téléphone mobile et souhaite utiliser la carte SIM de son téléphone pour être authentifié à la fois dans un réseau Wi-Fi et dans un réseau mobile, il doit alors transférer la carte SIM d'un terminal à l'autre. Ces
5 opérations de transfert s'avèrent peu aisées et ce d'autant plus que la carte SIM est au format "micro-SIM" de dimensions réduites.

Si l'utilisateur ne souhaite pas utiliser la carte SIM de son téléphone mobile, il doit se procurer une seconde carte SIM dédiée à l'authentification dans un
10 réseau Wi-Fi. Cette seconde carte représente un coût d'investissement et de gestion supplémentaire pour l'opérateur du réseau Wi-Fi. En outre, si l'utilisateur dispose de plusieurs terminaux Wi-Fi, il doit encore manipuler sa carte SIM pour la transférer d'un terminal à l'autre.

15 En outre, l'obtention d'une carte SIM et d'une carte PCMCIA d'interface n'est pas immédiate. Un utilisateur ne peut donc pas accéder à un réseau Wi-Fi instantanément à son arrivée dans la zone de couverture du réseau, sans avoir préalablement équipé son terminal d'un lecteur de carte SIM et introduit une carte SIM dans celui-ci.

20

Par ailleurs, dans les architectures décrites ci-avant, mettant en œuvre une carte SIM, la procédure d'authentification est effectuée à partir d'un terminal de type PC possédant un système d'exploitation ouvert et donc vulnérable. Il en résulte que la procédure d'authentification peut être facilement détournée à l'aide d'un
25 programme du type "cheval de Troie" installé frauduleusement dans le terminal et qui est conçu pour récupérer les informations d'authentification SIM de l'utilisateur, ces informations permettant ensuite d'établir des communications pirates dans un réseau mobile de type GSM.

30 La présente invention a pour but de supprimer 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.

Selon l'invention, ce procédé comprend des étapes consistant à transmettre les
35 données par une liaison sans fil entre le terminal 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.

Avantageusement, les données échangées entre le terminal et la carte à mémoire sont des données d'authentification d'un utilisateur et sont utilisées pour authentifier l'utilisateur lorsqu'il se connecte à un réseau de télécommunication à l'aide du terminal.

5

De préférence, le réseau de télécommunication est un réseau conforme à une norme 802.11x.

10 Egalement de préférence, la liaison sans fil est une liaison conforme au protocole Bluetooth.

L'invention concerne également un dispositif d'échange de données entre un terminal et une carte à mémoire accessible au terminal.

15 Selon l'invention ce dispositif comprend des moyens d'établissement d'une liaison sans fil entre le terminal et un terminal mobile équipé de la carte à mémoire, et des moyens pour échanger des données par la liaison sans fil entre le terminal et la carte à mémoire insérée dans le terminal mobile, le terminal mobile assurant la transmission des données entre la carte à mémoire et la
20 liaison sans fil.

Avantageusement, les données échangées entre le terminal et la carte à mémoire sont des données d'authentification d'un utilisateur, le dispositif comprenant des moyens pour utiliser les données échangées dans une procédure
25 d'authentification de l'utilisateur exécutée lorsqu'il se connecte à un réseau de télécommunication à l'aide du terminal,

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

Avantageusement, le module client et le module serveur sont conformes aux
35 spécifications SIM Access Profile.

Selon un mode de réalisation préféré de l'invention, le dispositif comprend, installé dans le terminal :

- un module implémentant un protocole d'authentification étendu aux cartes à mémoire,
- un module d'interface, conçu pour permettre à une application de dialoguer avec tout type de lecteur de carte à mémoire, par l'intermédiaire d'un pilote d'adaptation, et
- un pilote d'adaptation conçu pour accéder à la carte à mémoire insérée dans le terminal mobile, par l'intermédiaire de la liaison sans fil.

Avantageusement, le module d'interface est conforme aux spécifications du standard PC/SC.

Selon un mode de réalisation préféré de l'invention, le pilote d'adaptation est conçu pour accéder à un module client installé dans le terminal, 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.

De préférence, le dispositif comprend une mémoire d'échange par laquelle le pilote d'adaptation échange des informations avec le module client.

Un mode de réalisation préféré de l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux dessins annexés dans lesquels :

La figure 1 représente un système d'authentification sur la base d'une carte SIM d'un utilisateur connecté à un réseau Wi-Fi, selon l'art antérieur ;

La figure 2 représente les différentes couches logicielles mises en œuvre dans le poste d'utilisateur, selon l'art antérieur ;

La figure 3 représente un poste d'utilisateur connecté à un réseau Wi-Fi, et ayant accès à une carte SIM selon l'invention ;

La figure 4 représente les différentes couches logicielles mises en œuvre dans le poste d'utilisateur, selon l'invention ;

La figure 5 illustre sous la forme d'un organigramme certaines étapes du procédé selon l'invention.

La figure 3 représente un poste d'utilisateur selon l'invention. Ce poste utilisateur comprend un terminal Wi-Fi 1 équipé d'un module de communication 8 avec un réseau Wi-Fi 7 et ayant accès à une carte SIM 3 permettant à l'utilisateur d'être authentifié dans le réseau Wi-Fi.

5

Selon l'invention, la liaison entre le terminal 1 et la carte SIM est effectuée par l'intermédiaire d'une liaison sans fil 5, par exemple de type Bluetooth, entre le terminal 1 et un terminal mobile 2 dans lequel est insérée une carte SIM d'authentification du terminal mobile dans un réseau mobile.

10 De cette manière, l'utilisateur n'a pas besoin de disposer d'une carte SIM spécifique pour accéder à un réseau Wi-Fi ou de manipuler la carte SIM de son terminal mobile pour l'insérer dans un autre lecteur connecté à son terminal Wi-Fi.

15 Sur le plan logiciel, le terminal mobile 2 et le terminal Wi-Fi 1 mettent en œuvre un ensemble de protocoles et de procédures appelées SAP (SIM Access Profile) conçues dans le cadre du protocole Bluetooth pour donner accès à une carte SIM insérée dans un terminal par l'intermédiaire d'une liaison Bluetooth 5, d'une manière totalement transparente.

20

Ainsi, sur la figure 4, le terminal mobile 2 comprend un module serveur SAP 20 qui échange des messages d'un côté avec la carte SIM 3 par l'intermédiaire d'un lecteur 21 conforme à la norme ISO 7816-3, et de l'autre avec la liaison Bluetooth par l'intermédiaire d'une couche 22 implémentant le protocole RFCOMM (Serial Cable Emulation Protocol) émulant une liaison série, et une
25 couche de bas niveau 23 permettant d'établir une liaison radio Bluetooth 5 avec d'autres terminaux.

Selon l'invention, le terminal Wi-Fi 1 comprend un module client SAP 31, qui
30 communique avec le module serveur SAP 20 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 30.

35 Par ailleurs, l'authentification de l'utilisateur dans le réseau Wi-Fi est effectuée à l'aide d'un module EAP-SIM 24, ayant accès d'une part à un module de communication Wi-Fi 26 et à un module d'interface PC/SC 25 avec une carte SIM. Les modules EAP-SIM et PC/SC sont standards.

Le module d'interface PC/SC 25 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.

5 L'invention met en œuvre un pilote virtuel 27 conçu pour relayer et adapter les messages échangés entre le module d'interface 25 et le module client SAP 31, ces messages contenant des informations échangées avec la carte SIM 3. L'échange des messages entre le pilote virtuel et le client SAP est par exemple effectué à l'aide d'une mémoire d'échange ou de communication 28 dans

10 laquelle les messages à transmettre sont insérés.

Les modules SAP serveur 20 et client 31 ne font qu'échanger des messages avec la carte SIM, et lui appliquer des commandes, comme des commandes de mise sous/hors tension de la carte SIM.

15

Le module SAP client 31 est conçu pour exécuter une procédure de connexion avec le module SAP serveur 20 par l'intermédiaire d'une liaison Bluetooth, et une procédure de déconnexion. Lorsqu'une liaison est établie, le module SAP serveur 20 est conçu pour interroger le lecteur 21 de carte SIM et la carte SIM

20 susceptible d'être lue par le lecteur, et renvoyer au module SAP client des informations sur l'état du lecteur 21, 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

25 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 21. Le module SAP serveur est également conçu pour avertir le module SAP client de tous les événements de changement

30 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.

La procédure d'authentification 35 de l'utilisateur qui est exécutée pour accéder à un réseau Wi-Fi fait appel au module EAP-SIM 24. Ce module fait appel à

35 des fonctions d'accès et de commande de carte SIM, réalisées par le module d'interface PC/SC 25. Le module d'interface PC/SC est conçu pour communiquer avec plusieurs lecteurs de cartes à puce 39, par l'intermédiaire de pilotes 38 adaptés aux lecteurs. Le pilote virtuel 27 mis en œuvre par

l'invention est donc conçu comme un pilote 38.

- Pour communiquer avec plusieurs pilotes 27, 38, le module d'interface PC/SC comprend un module de gestion de ressources 37 et un module fournisseur de services 36. Le module de gestion de ressources 37 est conçu pour détecter les cartes à puces accessibles et rendre ces informations disponibles à plusieurs applications telles que l'application d'authentification 35. 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.
- 10 Le module fournisseur de services 36 est conçu pour offrir aux applications des fonctions de haut niveau, 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.
- 15 Sur la figure 5, le pilote virtuel 27 est conçu pour recevoir du module d'interface 25 des messages de transmission de commandes à appliquer à la carte SIM, ces messages provenant de l'application d'authentification 35, pour transmettre ces messages au module SAP client 31 pour que les commandes qu'ils contiennent soient finalement transmises à la carte à puce. Il est également conçu pour recevoir les réponses de la carte SIM et pour retransmettre ces réponses à l'application 35.
- 20 Plus précisément, lorsque le module d'interface 25 envoie une commande à appliquer à la carte SIM à l'étape 41, cette commande est reçue par le pilote virtuel 27 qui la stocke dans la mémoire d'échange 28 à l'étape 42. A l'étape suivante 43, le pilote virtuel notifie le module SAP client 31 de l'arrivée d'un message dans la mémoire d'échange, en générant un événement déclencheur, et se met en attente d'une notification d'événement. A l'étape suivante 44, le module SAP client qui est déclenché par l'événement généré par le pilote virtuel, lit la mémoire d'échange et transmet la commande lue à la carte SIM 3 par l'intermédiaire de la liaison Bluetooth et du module SAP serveur 20. A l'étape 45 suivante, cette commande est traitée par la carte SIM qui renvoie une réponse.
- 35 Chaque réponse de la carte SIM est transmise au module SAP client par le module SAP serveur et la liaison Bluetooth. A la réception de cette réponse à l'étape 46, le module SAP client inscrit cette réponse dans la mémoire

d'échange. A l'étape 47 suivante, il notifie le pilote virtuel de l'arrivée d'une réponse de la carte SIM à retransmettre en générant un événement déclencheur, et se met en attente d'un message à transmettre vers la carte SIM.

- 5 A l'étape suivante 48, le pilote virtuel est déclenché par l'événement généré par le module SAP client. Il lit alors la mémoire d'échange et transmet la réponse lue au module d'interface 25.

10 Les principales fonctions assurées par le pilote virtuel 27 sont donc les suivantes :

Transmit : cette fonction gère les échanges de messages avec la carte, c'est-à-dire reçoit des commandes venant de l'application d'authentification 35 et les envoie à la carte, puis renvoie la réponse de la carte SIM à l'application ; cette
15 fonction correspond donc aux étapes 42, 43 et 48.

Card Tracking : cette fonction informe l'application d'authentification du retrait ou de l'insertion, ou encore de la présence ou de l'absence de la carte SIM dans
20 le lecteur 21.

Card Reader Power : cette fonction permet de commander l'alimentation de la carte SIM ; lorsque la carte est mise sous tension, cette commande déclenche l'envoi par la carte d'un message contenant des informations sur son état.

25 Grâce à ces dispositions, la présence d'une liaison Bluetooth interposée sur la liaison avec la carte SIM est totalement transparente au module d'interface standard PC/SC 25. Par ailleurs, le pilote virtuel est vu par l'application EAP-SIM, comme un lecteur de carte à puce classique : l'architecture mise en place par l'invention ne modifie pas l'architecture existante faisant intervenir un
30 pilote 38 assurant l'interface entre d'un côté le terminal, et en particulier le module EAP-SIM 24 associé au module d'interface 25, et de l'autre, le lecteur de carte à puce 39 (figure 2).

En outre, les fonctionnalités du pilote virtuel 27 s'avèrent particulièrement simples étant donné que les messages gérés par le standard PC/SC
35 correspondent sensiblement aux messages prévus par les spécifications SAP.

Si la description qui précède décrit une application de l'invention à l'authentification d'un utilisateur dans un réseau Wi-Fi, il va de soi que

l'invention peut s'appliquer à l'authentification d'un utilisateur lorsqu'il se connecte à tout autre réseau et notamment à un réseau IP tel que le réseau Internet, lorsque le terminal utilisé ne dispose pas obligatoirement d'un lecteur de carte à puce. D'une manière plus générale, l'invention peut être utilisée pour

5 échanger des données avec une carte à mémoire.

REVENDEICATIONS

1. Procédé d'échange de données entre un terminal (1) et une carte à mémoire (3) accessible au terminal,
- 5 caractérisé en ce qu'il comprend des étapes consistant à transmettre les données par une liaison sans fil (5) entre le terminal (1) et un terminal mobile (2) équipé de la carte à mémoire (3), le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.
- 10 2. Procédé selon la revendication 1, caractérisé en ce que les données échangées entre le terminal (1) et la carte à mémoire (3) sont des données d'authentification d'un utilisateur et sont utilisées pour authentifier l'utilisateur lorsqu'il se connecte à un réseau de télécommunication (7) à l'aide du terminal (1).
- 15 3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le réseau de télécommunication (7) est un réseau conforme à une norme 802.11x.
- 20 4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que la liaison sans fil (5) est une liaison conforme au protocole Bluetooth.
- 25 5. Dispositif d'échange de données entre un terminal et une carte à mémoire (3) accessible au terminal, caractérisé en ce qu'il comprend des moyens (30, 20, 22, 23) d'établissement d'une liaison sans fil (5) entre le terminal (1) et un terminal mobile (2) équipé de la carte à mémoire (3), et des moyens pour échanger des données par la liaison sans fil entre le terminal et la carte à mémoire insérée dans le terminal
- 30 mobile, le terminal mobile assurant la transmission des données entre la carte à mémoire et la liaison sans fil.
- 35 6. Dispositif selon la revendication 5, caractérisé en ce que les données échangées entre le terminal (1) et la carte à mémoire (3) sont des données d'authentification d'un utilisateur, le dispositif comprenant des moyens pour utiliser les données échangées dans une procédure d'authentification de l'utilisateur exécutée lorsqu'il se connecte à un réseau de télécommunication (7) à l'aide du terminal (1),

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

5

8. Dispositif selon l'une des revendications 5 à 7,
caractérisé en ce que le réseau de télécommunication (7) est un réseau conforme
à une norme 802.11x.

10

9. Dispositif selon l'une des revendications 5 à 8,
caractérisé en ce qu'il comprend un module client (31) installé dans le terminal
(1) et un module serveur (20) installé dans le terminal mobile (2), conçus pour
établir des communications par l'intermédiaire de la liaison sans fil (5) entre le
terminal et la carte à mémoire (3) insérée dans le terminal mobile.

15

10. Dispositif selon la revendication 9,
caractérisé en ce que le module client (31) et le module serveur (20) sont
conformes aux spécifications SIM Access Profile.

20

11. Dispositif selon l'une des revendications 5 à 10,
caractérisé en ce qu'il comprend, installé dans le terminal (1) :

- un module (35) implémentant un protocole d'authentification étendu aux
cartes à mémoire,
- un module d'interface (25), conçu pour permettre à une application de
dialoguer avec tout type de lecteur de carte à mémoire, par l'intermédiaire
d'un pilote d'adaptation, et
- un pilote d'adaptation (27) conçu pour accéder à la carte à mémoire insérée
dans le terminal mobile (2), par l'intermédiaire de la liaison sans fil (5).

25

30

12. Dispositif selon la revendication 11,
caractérisé en ce que le module d'interface (25) est conforme aux spécifications
du standard PC/SC.

35

13. Dispositif selon la revendication 11 ou 12,
caractérisé en ce que le pilote d'adaptation (27) est conçu pour accéder à un
module client (31) installé dans le terminal (1), qui est conçu pour établir des
communications par l'intermédiaire de la liaison sans fil (5) avec un module
serveur (20) installé dans le terminal mobile (2) et ayant accès à la carte à

mémoire (3) insérée dans le terminal mobile.

14. Dispositif selon la revendication 13,
caractérisé en ce qu'il comprend une mémoire d'échange (28) par laquelle le
5 pilote d'adaptation (27) échange des informations avec le module client (31).

1/3

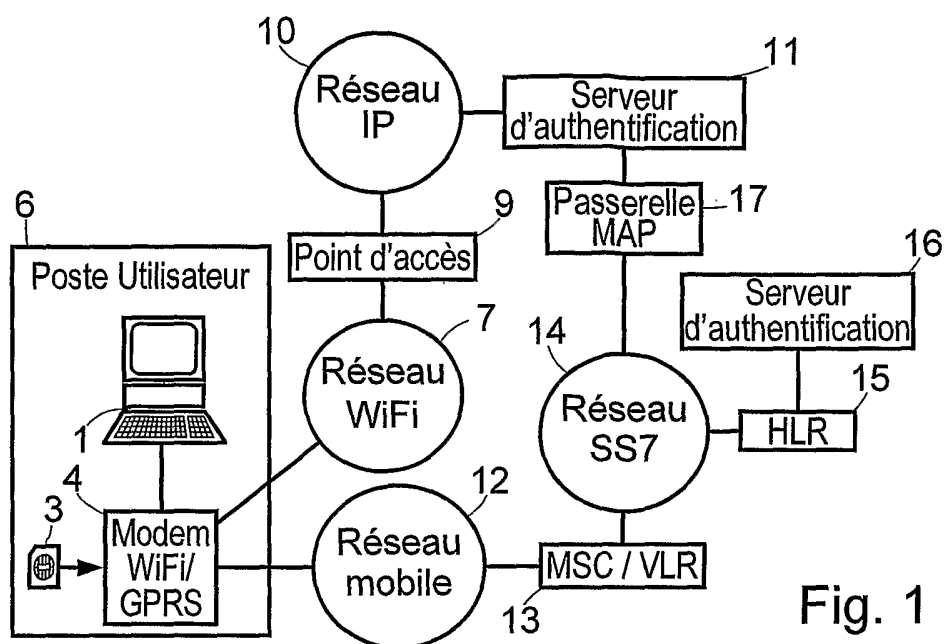


Fig. 1

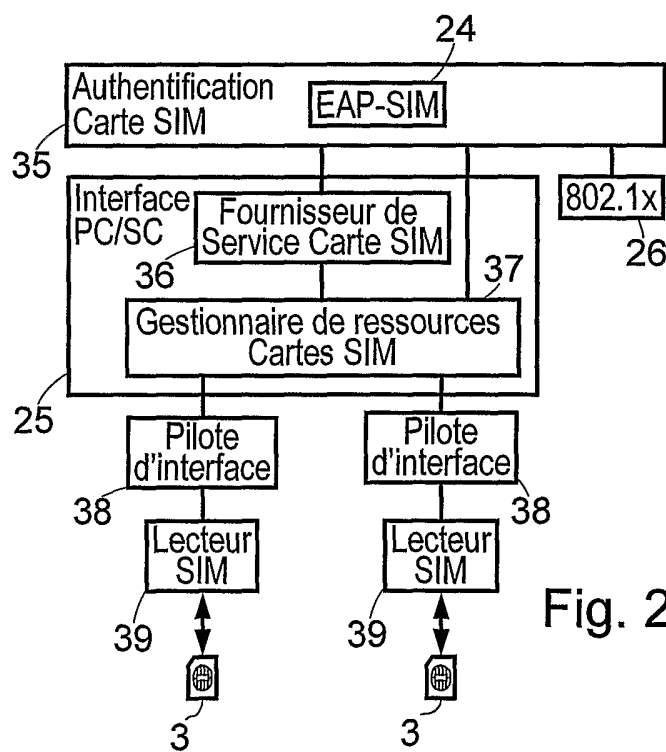


Fig. 2

2/3

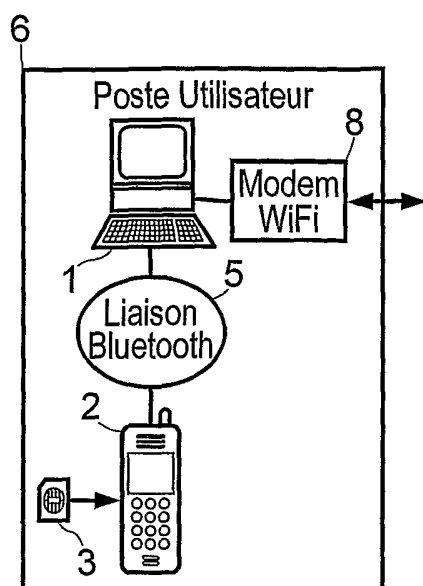
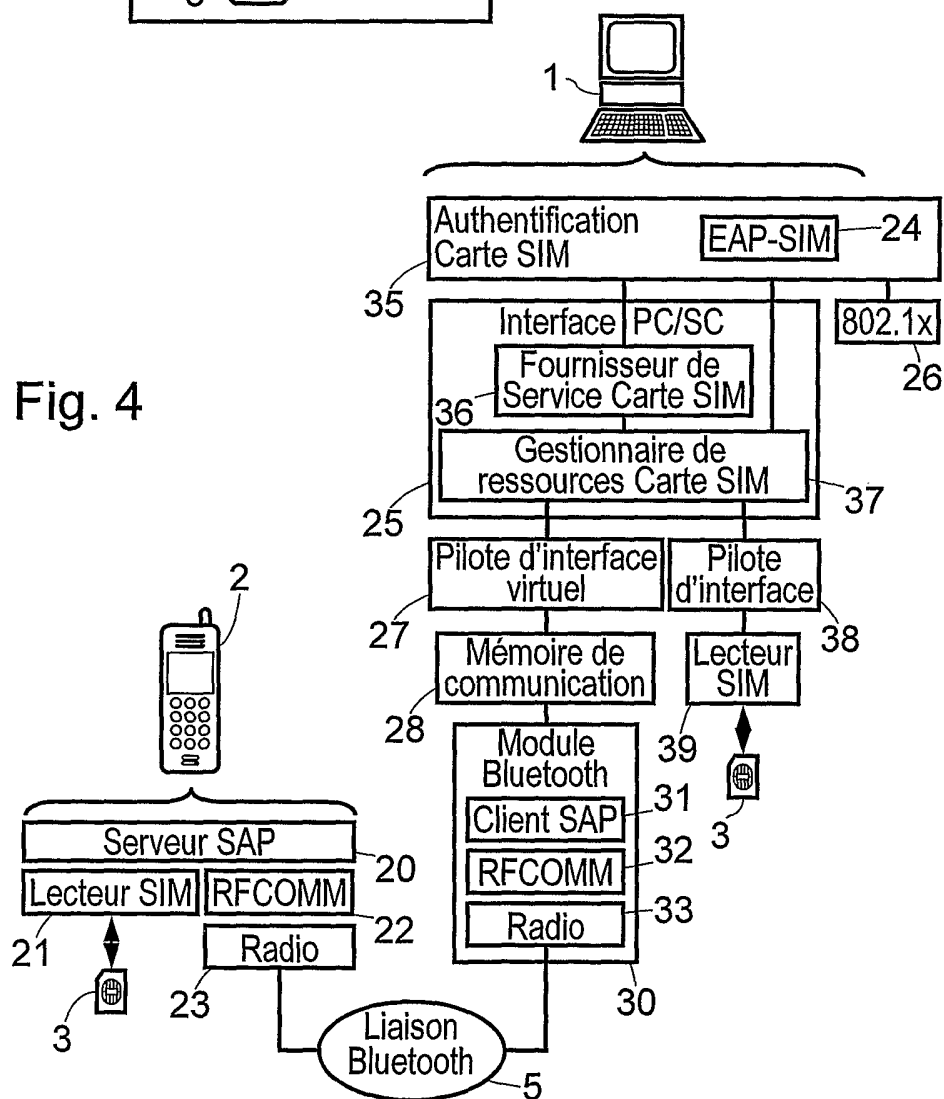


Fig. 3

Fig. 4



3/3

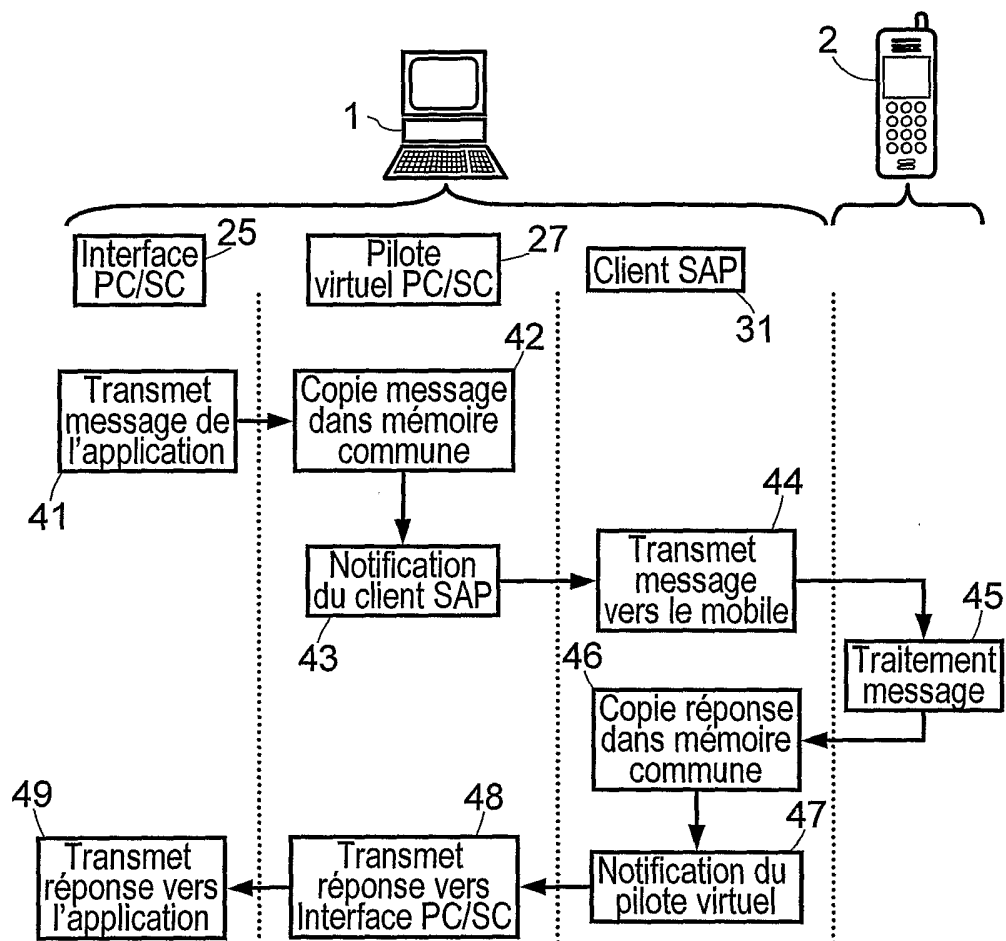


Fig. 5

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 03/02802

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28

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)

IPC 7 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	AHMAD A ET AL: "SIM-Based WLAN Authentication for Open Platforms" INTEL TECHNOLOGY JOURNAL, XX, US, 1 August 2003 (2003-08-01), pages 1-9, XP002271512 page 3, line 1 -page 8, line 30 --- -/--	1-14

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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

9 June 2004

Date of mailing of the international search report

03/08/2004

Name and mailing address of the ISA

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

Authorized officer

Wolf, W

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 03/02802

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP TSG SA WG3 SECURITY: "Technical Specification Group Service and System Aspects; Wireless Local Area Network (WLAN) Interworking Security; (Release 6)" 3RD GENERATION PARTNERSHIP PROJECT, 'Online! 8 - 11 October 2002, pages 1-31, XP002283825 Munich Retrieved from the Internet: <URL:www.3gpp.org> 'retrieved on 2004-06-09! paragraph '4.1.2! page 11, paragraph 6.1 -page 17, paragraph 6.2	1,5
X	----- US 2002/169966 A1 (NYMAN KAI ET AL) 14 November 2002 (2002-11-14) paragraphs '0006!-'0013! paragraphs '0015!-'0027! -----	1,2,5,6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 03/02802

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002169966 A1	14-11-2002	US 2002169958 A1	14-11-2002
		EP 1397932 A1	17-03-2004
		WO 02093967 A1	21-11-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 03/02802

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L12/28

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)

CIB 7 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 réalisable, 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	AHMAD A ET AL: "SIM-Based WLAN Authentication for Open Platforms" INTEL TECHNOLOGY JOURNAL, XX, US, 1 août 2003 (2003-08-01), pages 1-9, XP002271512 page 3, ligne 1 -page 8, ligne 30 --- -/--	1-14



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'appartenant 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention 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

9 juin 2004

Date d'expédition du présent rapport de recherche internationale

03/08/2004

Nom et adresse postale de l'administration chargée de la recherche internationale

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

Fonctionnaire autorisé

Wolf, W

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 03/02802

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	3GPP TSG SA WG3 SECURITY: "Technical Specification Group Service and System Aspects; Wireless Local Area Network (WLAN) Interworking Security; (Release 6)" 3RD GENERATION PARTNERSHIP PROJECT, 'en ligne! 8 - 11 octobre 2002, pages 1-31, XP002283825 Munich Extrait de l'Internet: <URL:www.3gpp.org> 'extrait le 2004-06-09! alinéa '4.1.2! page 11, alinéa 6.1 -page 17, alinéa 6.2 ----	1,5
X	US 2002/169966 A1 (NYMAN KAI ET AL) 14 novembre 2002 (2002-11-14) alinéas '0006!-'0013! alinéas '0015!-'0027! -----	1,2,5,6

PT/FR 03/02802

Formulaire PCT/ISA/210 (annexe familles de brevets) (Janvier 2004)