

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 20.11.97.

30 Priorité :

43 Date de mise à la disposition du public de la  
demande : 21.05.99 Bulletin 99/20.

56 Liste des documents cités dans le rapport de  
recherche préliminaire : *Se reporter à la fin du  
présent fascicule*

60 Références à d'autres documents nationaux  
apparentés :

71 Demandeur(s) : GEMPLUS SOCIETE EN COMMAN-  
DITE PAR ACTIONS — FR.

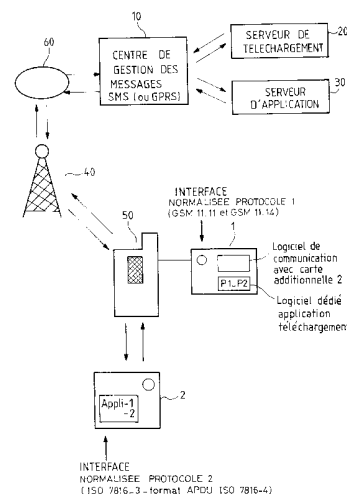
72 Inventeur(s) : BEAUJARD OLIVIER et IMBERT  
PATRICK.

73 Titulaire(s) :

74 Mandataire(s) : CABINET BALLOT SCHMIT.

54 PROCEDE, CARTE A PUCE ET TERMINAUX POUR EFFECTUER DES TRANSACTIONS A TRAVERS UN  
RESEAU DE TELECOMMUNICATION.

57 L'invention concerne un procédé pour effectuer des transactions à travers un réseau de télécommunication (60) au moyen de cartes à puce (1, 2) et de terminaux de télécommunication (50) munis d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir une carte à puce d'identification d'abonné (1) dédiée à la téléphonie, l'autre pour recevoir une carte à puce (2) dédiée à une ou plusieurs applications autres que la téléphonie. Il est prévu selon l'invention d'introduire des moyens de communication à toute carte d'identification d'abonné (1) pour lui permettre de piloter toute carte applicative (2) à travers le terminal de télécommunication (50).



**PROCÉDÉ, CARTE A PUCE ET TERMINAUX POUR EFFECTUER DES  
TRANSACTIONS A TRAVERS UN RÉSEAU DE TÉLÉCOMMUNICATION**

L'invention concerne un procédé pour effectuer des transactions à travers un réseau de télécommunications au moyen de cartes à puce et de terminaux de télécommunication.

5 Elle concerne également les cartes à puce et les terminaux permettant de mettre en oeuvre le procédé.

Elle trouve de nombreuses applications dans les transactions monétaires, le porte-monnaie électronique, les transactions relatives à la santé, aux jeux.

10 Les réseaux de télécommunications concernés sont tous les réseaux susceptibles d'être empruntés par un abonné du téléphone pour accéder à un autre abonné ou à des services.

15 Parmi ces réseaux on peut citer les réseaux de téléphonie, réseau commuté ou réseau à intégration de services et le réseau de téléphonie cellulaire.

La nouvelle génération de terminaux de télécommunication prévoit que ces terminaux soient équipés de deux interfaces de lecture de cartes à puce, 20 l'une pour communiquer avec une carte à puce d'identification d'abonné dédiée à la téléphonie telles que par exemple les cartes SIM (Subscriber Identity Module) dans le cas du système de télécommunication cellulaire et l'autre pour une carte à puce (carte 25 applicative) dédiée à une ou plusieurs applications autres que la téléphonie. Il pourra s'agir par exemple d'une carte porte-monnaie électronique.

Les cartes à puce dédiées à une ou plusieurs applications autres que la téléphonie peuvent être 30 délivrées par des opérateurs complètement indépendants

et la communication avec ces cartes applicatives est établie selon des protocoles distincts.

Il s'avère nécessaire par conséquent que cette nouvelle génération de terminaux de télécommunication  
5 supporte les jeux de commandes applicatifs de ces différents types de cartes applicatives (par exemple application bancaire, application fidélité).

Ceci est très contraignant pour les prestataires de services qui doivent de ce fait se lier à un fabricant  
10 de terminaux pour proposer leur applications à leurs clients.

De plus cela impose une limitation dans le choix des cartes applicatives utilisables avec un terminal de télécommunication donné, à celles qui auront été  
15 prévues initialement sous peine d'avoir à modifier les logiciels du terminal.

La présente invention permet de remédier à ces problèmes.

20 L'invention a comme premier objectif de ne pas alourdir les interfaces logiques de communication du terminal tout en lui permettant d'accepter n'importe quelle carte applicative et ceci en introduisant des moyens de communication à toute carte d'identification  
25 d'abonné dédiée à la téléphonie pour lui permettre de piloter toute carte applicative à travers le terminal de télécommunication.

L'invention a plus particulièrement pour objet un procédé pour effectuer des transactions à travers un  
30 réseau de télécommunication au moyen de cartes à puce et de terminaux de télécommunication d'accès au réseau munis d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir une carte à puce d'identification d'abonné dédiée à la téléphonie,

l'autre pour recevoir une carte à puce additionnelle dédiée à une ou plusieurs applications autres que la téléphonie; caractérisé en ce que la carte à puce d'identification d'abonné communique avec la carte additionnelle via le terminal, au moyen d'un jeu de commandes destinées à piloter ladite carte additionnelle, ces commandes étant pré-formatées par la carte d'identification d'abonné selon le format du protocole de communication de la carte additionnelle et transmises par le terminal selon le protocole de transport de ce dernier.

L'invention a également pour objet une carte à puce téléphonique d'identification d'abonné, caractérisé en ce qu'elle comporte des moyens de communication avec une carte additionnelle dédiée à une ou plusieurs applications autres que la téléphonie, via un terminal de télécommunication muni d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir la carte à puce d'identification d'abonné dédiée à la téléphonie et l'autre pour recevoir la carte à puce additionnelle, ces moyens comprenant un jeu de commandes destinées à piloter la carte additionnelle, ledites commandes étant pré-formatées par la carte d'identification d'abonné selon le format (APDU) du protocole de communication de la carte additionnelle et transmises par le terminal selon le protocole de transport de ce dernier.

L'invention a aussi pour objet un terminal de télécommunication d'accès au réseau muni d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir une carte à puce d'identification d'abonné dédiée à la téléphonie, l'autre pour recevoir une carte à puce additionnelle dédiée à une ou plusieurs applications autres que la téléphonie, caractérisé en ce qu'il comporte:

- des moyens adaptés pour recevoir des commandes émises par la carte d'identification d'abonné selon le protocole de transport dudit terminal et destinées à piloter la carte additionnelle, ledites commandes étant  
5 pré-formatées par la carte d'identification d'abonné selon le format du protocole de communication de la carte additionnelle,

- des moyens pour transmettre parmi ces commandes les commandes "envoi commande entrante/sortante carte  
10 2" à la carte additionnelle telles que pré-formatées,

- des moyens pour exécuter parmi ces commandes les commandes "allume/éteint carte 2",

- des moyens pour émettre une commande "carte 2 présente" à la carte d'identification d'abonné.  
15

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description qui est faite ci-après et qui est donnée à titre d'exemple illustratif et non limitatif en regard des figures sur  
20 lesquelles :

- la figure 1, représente schématiquement une vue globale d'un réseau de télécommunication pour la mise en oeuvre du procédé de l'invention,

- la figure 2, représente de manière plus détaillé  
25 de façon schématique, une carte d'identification d'abonné et une carte additionnelle.

- la figure 3, illustre de façon détaillée les échanges entre les différents éléments du système dans le cas d'une commande entrante ou sortante conformément  
30 au procédé.

- la figure 4, illustre de façon plus générale les échanges entre les différents éléments pour toutes les commandes.

Comme cela a été dit, le principe de l'invention s'applique à tout type de réseau de téléphonie, réseau téléphonique commuté, RNIS, cellulaire (GSM). Mais la description qui va suivre est donnée pour un réseau de télécommunication cellulaire dont les terminaux sont des radio-téléphones mobiles.

Selon cet exemple illustré par la figure 1 le système comporte :

- un centre de gestion 10 des messages SMS (Short Message Service Center) ou GPRS (Global Packet Radio Service);

- un serveur 20 de téléchargement contenant les programmes dédiés à la mise en oeuvre d'applications,

- un serveur d'application 30 : porte monnaie électronique, banque, points de fidélité donnés par un commerçant;

- un réseau GSM 60 contenant au moins une borne cellulaire 40. Chaque borne permet à l'utilisateur d'être connecté au réseau de l'opérateur;

- un téléphone mobile 50 de l'utilisateur. Un téléphone mobile est composé d'une antenne de réception, d'une batterie, d'un écran de visualisation, d'un clavier, d'une ou plusieurs interfaces cartes, d'un microprocesseur contenant un logiciel système.

Dans la présente invention, le téléphone mobile est muni de deux interfaces carte à puce.

- une carte d'identification d'abonné 1 dénommée carte SIM. Cette carte est présente dans le téléphone mobile de l'utilisateur et lui permet d'être identifié par l'opérateur de téléphonie cellulaire.

- une carte additionnelle 2 dite carte applicative car elle est destinée à des applications d'un type autre que l'application de la carte SIM. Ces

applications peuvent être des applications porte monnaie électronique, banque, points de fidélité.

5 La figure 2 représente les éléments contenus dans la carte SIM 1 et dans la carte additionnelle 2 afin de mettre en oeuvre l'invention.

La carte SIM 1 comporte un microprocesseur, une mémoire morte (ROM), d'une mémoire vive (RAM) et d'une mémoire de type EEPROM. La mémoire morte (ROM) et la  
10 mémoire EEPROM contiennent des logiciels et des données permettant le fonctionnement de la carte SIM. Il s'agit notamment d'un logiciel système et d'un ou plusieurs programmes P1-P2 téléchargés, dédiés à la mise en oeuvre d'applications par la carte additionnelle.  
15 Chaque programme dédié à la mise en oeuvre d'application comporte une ou plusieurs applications pour la carte additionnelle. Ces applications correspondent à la gestion de l'interface homme machine avec l'utilisateur, à la gestion de la communication avec la carte additionnelle et la gestion de la  
20 communication avec le serveur d'application 30 lié à la carte additionnelle.

Le logiciel de communication de la carte SIM utilise le jeu de commandes que possède la carte SIM  
25 pour dialoguer avec la carte additionnelle 2 à travers le terminal.

Ce jeu de commande comporte des commandes pré-formatées selon le format APDU (ISO 7816-4) qui est le format du protocole de communication de la carte 2. Ces  
30 commandes sont encapsulées par la carte SIM suivant le protocole de transport GSM 11.14 et transmises suivant ce protocole par le terminal (les commandes émises par la carte SIM sont lues par le terminal).

Plus précisément la carte SIM 1 dispose des quatre commandes suivantes :

- a) - "allume carte 2"
- b) - "éteint carte 2"
- 5 c) - "envoi commande entrante dans la carte 2"
- d) - "envoi commande sortante dans la carte 2"

Les deux premières a), b), sont exécutées par le terminal, les deux autres c) et d) sont communiquées au format APDU à la carte 2.

10 Un schéma illustrant de façon plus détaillée les différents échanges est illustré dans la suite à propos de la figure 3.

La carte additionnelle 2, (carte applicative) est composée d'un microprocesseur, d'une mémoire morte (ROM), d'une mémoire vive (RAM) et d'une mémoire de type EEPROM. La mémoire morte (ROM et la mémoire EEPROM  
15 contiennent des logiciels et des données permettant le fonctionnement de cette carte applicative, notamment un logiciel système et des logiciels applicatifs ( par exemple un logiciel de porte-monnaie électronique, et/ou un logiciel de gestion de points de fidélité...)).

20 Le terminal qui est un téléphone mobile selon cet exemple permet l'insertion de 2 cartes. Pour cela il comporte deux interfaces de lecture de carte à puce. La première interface permet l'insertion de la carte SIM  
25 identifiant l'utilisateur du téléphone sur le réseau auquel il est connecté. La ou les interfaces cartes supplémentaires permettent à l'utilisateur d'insérer des cartes d'un autre type (carte bancaire, carte de  
30 fidélité, carte santé, ...).

Le terminal comporte en outre des éléments non représentés tel qu'un microprocesseur et une mémoire de programme contenant un logiciel système et un logiciel communication.



Ce logiciel communication est apte selon l'invention à recevoir les commandes émises par la carte SIM.

5 Ce logiciel permet en outre, de transmettre à la carte 2 les commandes entrante/sortante carte 2 telles que pré-formatées c'est à dire de les transmettre au format APDU, d'exécuter les commandes allume/éteint carte 2 et d'émettre une commande "carte 2 présente" à la carte SIM dès que le téléphone mobile a détecté la présence d'une carte 2 dans son lecteur. La détection  
10 peut être mécanique ou électrique. Cette commande est envoyée à la carte SIM selon le protocole de communication GSM 11.14.

15 On va maintenant détailler le dialogue entre les éléments du système à partir du schéma de la figure 3 dans le cas d'une commande entrante ou sortante émise par la carte SIM pour la carte additionnelle 2. Une commande entrante est typiquement une commande  
20 d'écriture donnée à la carte 2, cette commande est accompagnée des données à écrire.

Une commande sortante est typiquement une commande de lecture donnée à la carte 2.

. à l'étape I, la carte SIM encapsule la commande  
25 de format APDU (ISO-7816-4) dans une commande SIM TOOLKIT de la norme GSM 11.14,

. à l'étape II, le terminal récupère la commande APDU et la communique à la carte additionnelle 2,

. à l'étape III, la carte additionnelle 2 renvoie  
30 au terminal un code retour SW1/SW2 au format APDU. Ce code est assorti de données dans le cas d'une commande sortante,

. à l'étape IV, le terminal prépare le "Terminal Response" TR et envoie à la carte SIM la réponse avec le code retour,

5 . à l'étape V, la carte SIM traite la réponse dans le cas d'une bonne réception sinon recommence à partir de l'étape I.

10 La figure 4 illustre les commandes essentielles utilisées pour établir un dialogue entre la carte SIM et la carte additionnelle - carte 2 - à travers le terminal.

15 La commande "carte 2 présente" est émise par le terminal. Les quatre autres commandes sont émises par la carte SIM pour le terminal qui vient les lire. La commande "Allume Carte 2" est exécutée par le terminal et se traduit par une ordre RESET envoyé à la carte 2. La commande "Eteint carte 2" est exécutée par le terminal, qui pour cela n'alimente plus en courant la carte 2.

20 Les commandes Entrante/Sortante carte 2 ont déjà été détaillées à partir du schéma de la figure 3.

## REVENDICATIONS

1. Procédé pour effectuer des transactions à travers un réseau de télécommunication (60) au moyen de cartes à puce (1,2) et de terminaux de télécommunication (50) d'accès au réseau munis d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir une carte à puce d'identification d'abonné (1) dédiée à la téléphonie, l'autre pour recevoir une carte à puce additionnelle (2) dédiée à une ou plusieurs applications autres que la téléphonie; caractérisé en ce que la carte à puce d'identification d'abonné communique avec la carte additionnelle via le terminal, au moyen d'un jeu de commandes destinées à piloter ladite carte additionnelle, ces commandes étant pré-formatées par la carte d'identification d'abonné selon le format du protocole de communication de la carte additionnelle et transmises par le terminal selon le protocole de transport de ce dernier.

2. Procédé pour effectuer des transactions selon la revendication 1, caractérisé en ce que le jeu de commandes comporte au moins les commandes suivantes:

- mise sous tension de la carte additionnelle "allume carte 2",
- mise hors tension de la carte additionnelle "éteint carte 2",
- envoi de données dans carte additionnelle "Envoie commande entrante dans carte 2",
- réception de données de la carte additionnelle "Envoie commande sortante dans carte 2".

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que la communication avec la carte additionnelle (2) via le terminal comporte une commande supplémentaire envoyée par le terminal à la carte d'identification d'abonné selon le protocole de communication de celle-ci, cette commande étant :

- présence de la carte additionnelle "carte 2 présente".

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la communication avec la carte additionnelle (2) via le terminal est mise en oeuvre par un programme chargé dans une mémoire de programme de la carte d'identification d'abonné.

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la carte d'identification d'abonné (1) est apte à piloter le téléchargement à travers le terminal, dans sa propre mémoire de programme, d'un ou plusieurs programmes dédiés à la mise en oeuvre d'applications pour la carte additionnelle (2), ces programmes dédiés provenant d'un serveur de téléchargement d'applications accessible par les terminaux au moyen du réseau de télécommunication.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le réseau téléphonique (60) est le réseau de radio téléphonie mobile (GSM), les terminaux étant des radio téléphones et les cartes d'identification d'abonné étant des cartes SIM.

7. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le réseau téléphonique est le réseau commuté de téléphonie ou le réseau à intégration de service (RNIS).

5

8. Carte à puce téléphonique d'identification d'abonné, caractérisé en ce qu'elle comporte des moyens de communication avec une carte additionnelle (2) dédiée à une ou plusieurs applications autres que la  
10 téléphonie, via un terminal de télécommunication (50) muni d'au moins deux interfaces de lecture de cartes à puce, l'une pour recevoir la carte à puce d'identification d'abonné dédiée à la téléphonie et l'autre pour recevoir la carte à puce additionnelle,  
15 ces moyens comprenant un jeu de commandes destinées à piloter la carte additionnelle (2), ledites commandes étant pré-formatées par la carte d'identification d'abonné selon le format (APDU) du protocole de communication de la carte additionnelle et transmises  
20 par le terminal selon le protocole de transport de ce dernier.

9. Carte à puce téléphonique d'identification d'abonné selon la revendication 8, caractérisé en ce  
25 qu'elle comporte une mémoire de programme comportant un programme adapté pour piloter le téléchargement à travers le terminal (50), dans cette mémoire, d'un ou plusieurs programmes dédiés à la mise en oeuvre d'applications pour la carte additionnelle (2), ces  
30 programmes provenant d'un serveur de téléchargement (20), accessible par les terminaux au moyen du réseau de télécommunication (60).

10. Carte à puce téléphonique d'identification d'abonné selon la revendication 9, caractérisé en ce que les programmes dédiés téléchargés dans la carte d'identification d'abonné (1) comportent une ou  
5 plusieurs applications pour la carte additionnelle (2), ces applications correspondant à la gestion de l'interface homme machine avec l'utilisateur, la gestion de la communication avec ladite carte additionnelle et la gestion de la communication avec le  
10 serveur d'application (30) lié à la carte additionnelle.

11. Terminal de télécommunication d'accès au réseau muni d'au moins deux interfaces de lecture de cartes à  
15 puce, l'une pour recevoir une carte à puce d'identification d'abonné (1) dédiée à la téléphonie, l'autre pour recevoir une carte à puce additionnelle (2) dédiée à une ou plusieurs applications autres que la téléphonie, caractérisé en ce qu'il comporte:

20 - des moyens adaptés pour recevoir des commandes émises par la carte d'identification d'abonné selon le protocole de transport dudit terminal et destinées à piloter la carte additionnelle, ledites commandes étant pré-formatées par la carte d'identification d'abonné  
25 selon le format (APDU) du protocole de communication de la carte additionnelle,

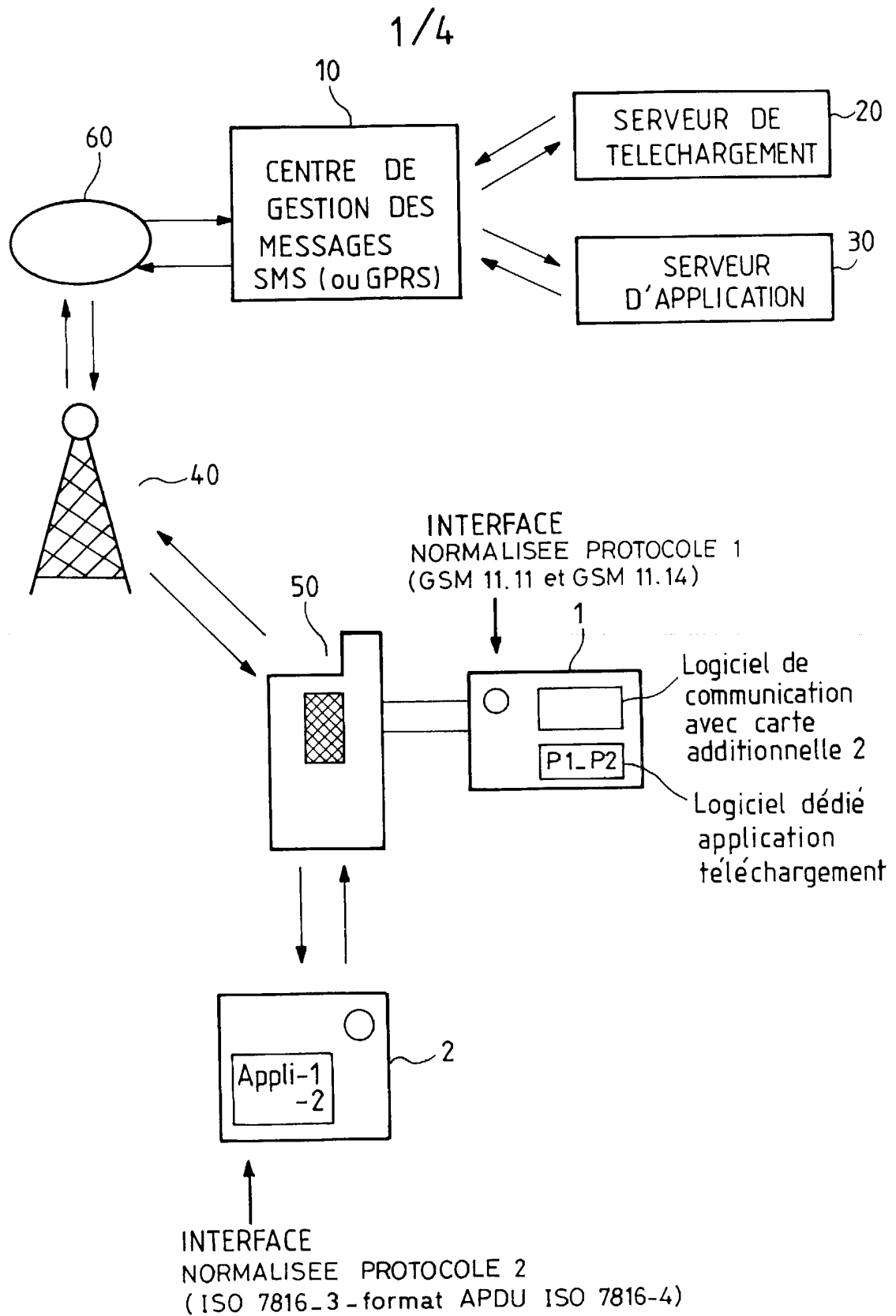
- des moyens pour transmettre parmi ces commandes les commandes "envoie commande entrante/sortante carte 2" à la carte additionnelle telles que pré-formatées,

30 - des moyens pour exécuter parmi ces commandes les commandes "allume/éteint carte 2",

- des moyens pour émettre une commande "carte 2 présente" à la carte d'identification d'abonné.

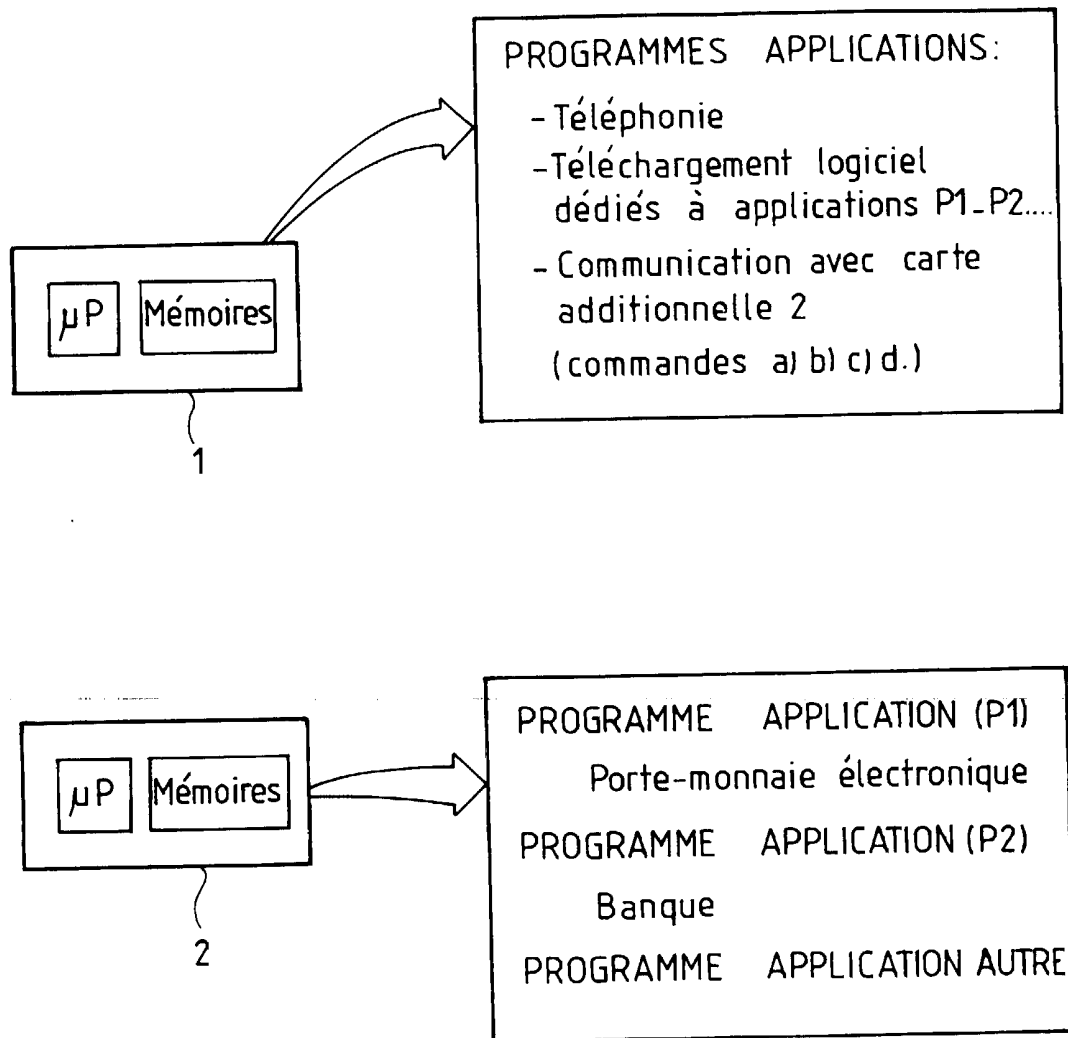
12. Terminal de télécommunication selon la revendication 11, caractérisé en ce que les commandes émises par la carte d'identification d'abonné (1) sont encapsulées selon le protocole de transport du terminal de télécommunication, le terminal étant apte à récupérer les données pré-formatées ainsi reçues pour les transmettre à la carte additionnelle selon son protocole de communication.

10 13. Terminal de téléphonie selon la revendication 11, caractérisé en ce que le protocole de transport entre le terminal et la carte d'identification d'abonné est définie par la norme GSM 11.14 et en ce que le protocole de communication avec la carte additionnelle  
15 suit le format APDU (ISO 7816-4).

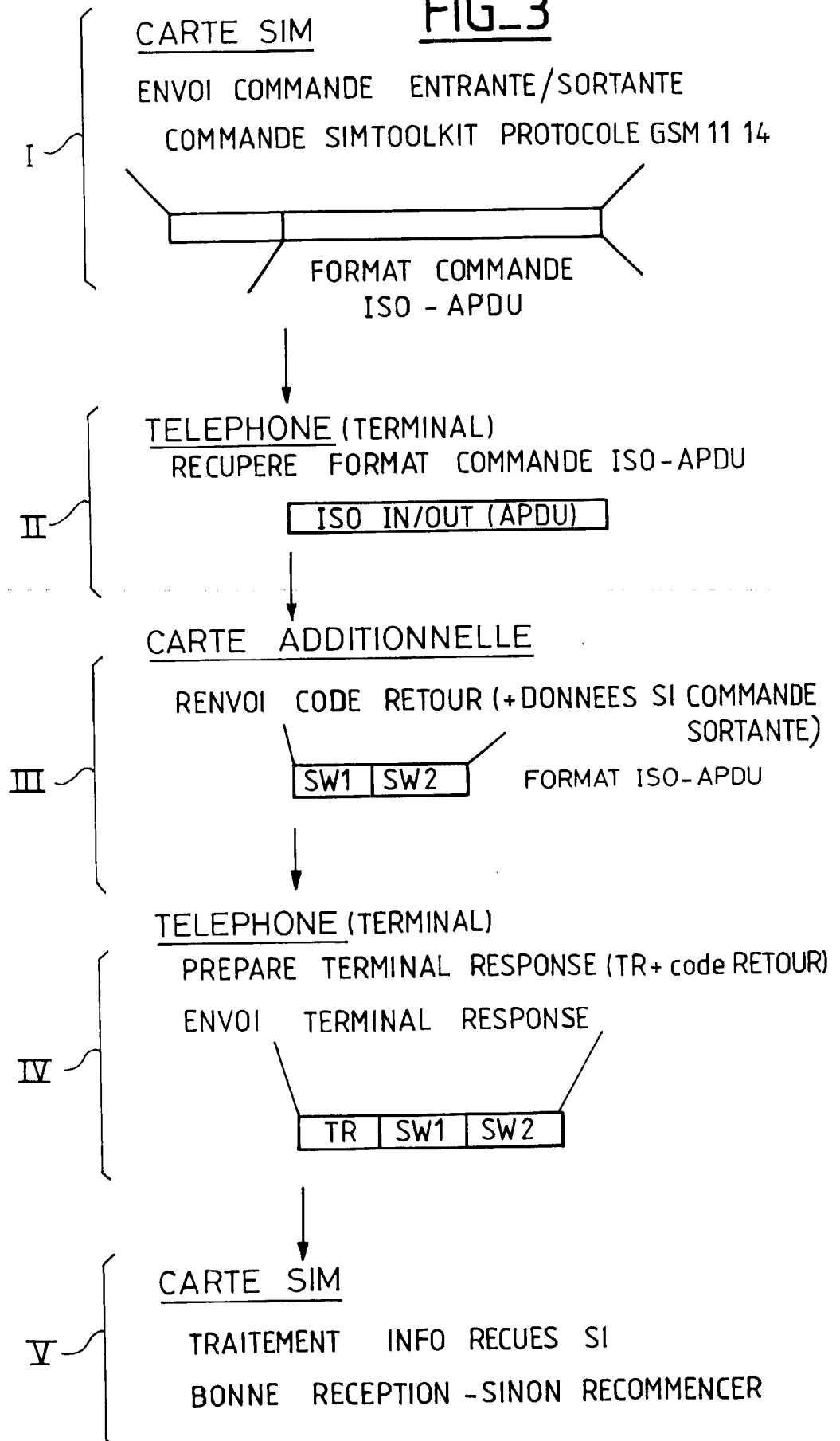
FIG\_1



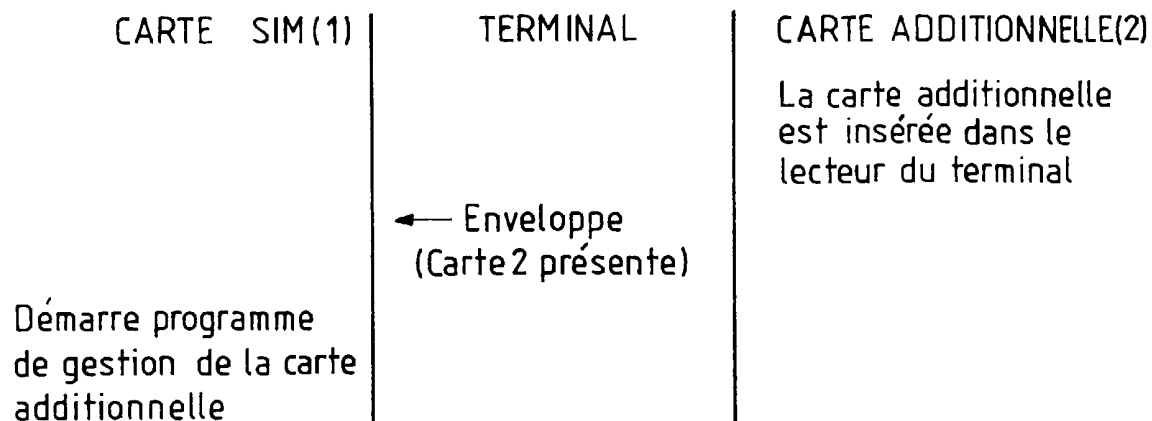
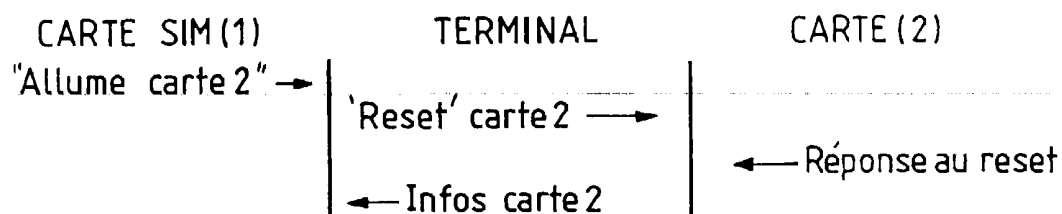
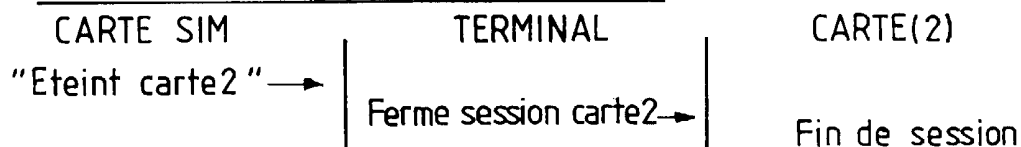
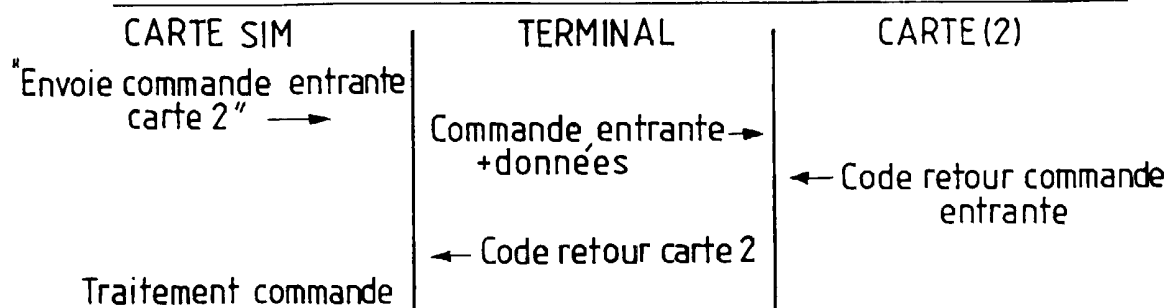
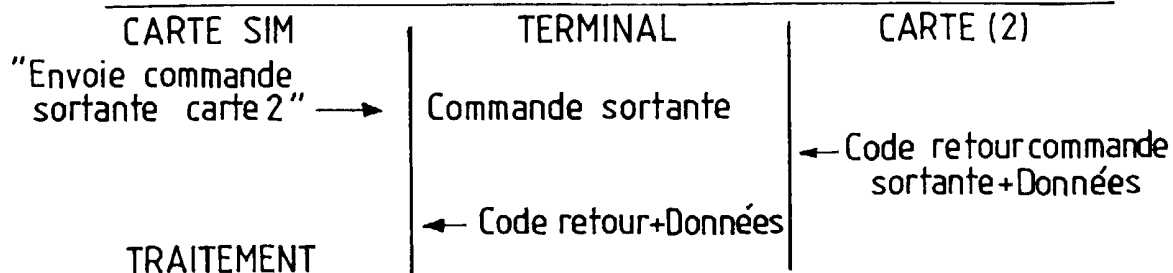
2/4

FIG\_2

3/4

FIG\_3

4/4

FIG\_4• COMMANDE "CARTE 2 PRESENTE"• COMMANDE "ALLUME CARTE 2"• COMMANDE "ETEINT CARTE 2"• COMMANDE "ENVOIE COMMANDE ENTRANTE CARTE 2"• COMMANDE "ENVOIE COMMANDE SORTANTE CARTE 2"

INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

**RAPPORT DE RECHERCHE  
PRELIMINAIRE**  
établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

N° d'enregistrement  
national

FA 554153  
FR 9714578

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	DE 295 20 925 U (PHILIPS PATENTVERWALTUNG) 17 octobre 1996 * le document en entier *	1,6,8,11
A	US 5 227 615 A (Y. OOGITA) 13 juillet 1993 * le document en entier *	1,8,11
A	EP 0 355 372 A (SYSPATRONIC) 28 février 1990 * abrégé; revendications; figures * * colonne 4, ligne 18 - colonne 5, ligne 51 *	1,3-5, 8-11
A	WO 97 05729 A (TELECOM ITALIA MOBILE) 13 février 1997	
A	FR 2 729 523 A (SOLAIC) 19 juillet 1996	
A	GB 2 269 512 A (NOKIA MOBILE PHONES) 9 février 1994	
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		G07F G06K H04M
Date d'achèvement de la recherche		Examineur
22 octobre 1998		David, J
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons &amp; : membre de la même famille, document correspondant</p>		