

①②

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 20.12.99.

③⑦ Priorité :

④③ Date de mise à la disposition du public de la
demande : 22.06.01 Bulletin 01/25.

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

⑥⑦ Références à d'autres documents nationaux
apparentés :

⑦① Demandeur(s) : ALCATEL Société anonyme — FR.

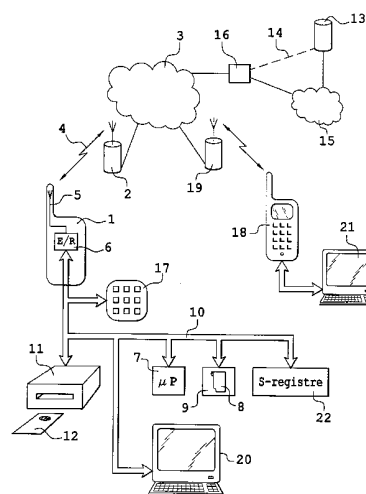
⑦② Inventeur(s) : TISSERAND BRUNO et DAVIT LUC.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) : COMPAGNIE FINANCIERE ALCA-
TEL.

⑤④ PROCÉDE DE TRANSMISSION DE MINI-MESSAGES ET SON DISPOSITIF ASSOCIÉ.

⑤⑦ Pour réduire un coût de communication dans le cas de messages utilisateurs de quelques dizaines d'octets à travers un réseau (3) de téléphonie mobile et pour éviter d'avoir à établir un canal de communication comme dans le cas de transmissions de données de plusieurs milliers d'octets, alors on utilise des champs disponibles dans des messages de signalisations pour transporter ces messages utilisateurs, une communication se faisant alors par l'intermédiaire des messages de signalisations et sans qu'un canal de communication dédié ne soit établi.



Procédé de transmission de mini-messages et son dispositif associé

La présente invention a pour objet un procédé de transmission de mini-messages. Elle a également pour objet un dispositif d'émission et/ou de réception associé. L'invention s'applique au domaine des transmissions de données à travers un réseau de transmission. Elle s'applique plus particulièrement au domaine des transmissions où le réseau de transmission de données est un réseau de téléphonie mobile ou un réseau numérique à intégration de service, ou encore RNIS. Le but de l'invention est de transmettre des mini-messages, à travers le réseau de transmission, entre un appelant et un appelé et ce à moindre coût. Cependant, une application préférée de l'invention concerne la transmission d'un code de carte à puce à un centre d'authentification en utilisant comme réseau de transmission un réseau de téléphonie mobile.

Actuellement, on sait émettre un message d'un appelant vers un appelé à travers un réseau de transmission, un message étant une structure de données comportant de quelques octets voire quelques dizaines d'octets, on parlera alors de mini-messages, à plusieurs milliers d'octets. Pour émettre un message, il est nécessaire, dans l'état de la technique, d'établir une liaison de communication entre un appelant et un appelé, de transmettre ce message à travers cette liaison et enfin de supprimer cette liaison de communication une fois l'échange entre l'appelant et l'appelé terminé.

Une telle réalisation, dans le cas de l'émission de mini-messages, présente des problèmes. En effet, en se ramenant à l'échelle d'un mini-message, une durée nécessaire à l'établissement de la liaison de communication ajoutée à une durée de la communication ajoutée encore à la durée de la suppression de la liaison de communication donne une durée de transmission trop contraignante.

En outre, dans le cas où les mini-messages sont des codes de cartes à puce par exemple, on peut avoir plusieurs dizaines de milliers de transactions, à travers le réseau de transmission, chaque jour. Ce nombre élevé de transactions associé au mode de réalisation selon l'état de la technique conduit à une charge du réseau qui est tout à fait conséquente. Cette charge du réseau de transmission est appelée à augmenter de plus en plus suite à l'augmentation toujours croissante d'applications mettant en

œuvre une carte à puce ainsi qu'un nombre de transactions associées. Il est à préciser, en outre, que l'utilisation d'une liaison de communication à travers un réseau de transmission n'est pas gratuite. Il s'ensuit un coût non négligeable, vu le nombre de transactions, pour l'envoi de mini-messages.

5 La présente invention a pour objet de remédier à ces problèmes en proposant un procédé de transmission de tels mini-messages. Le procédé de l'invention permet de réduire le délai de transmission à une valeur la plus faible possible et ce en transmettant des données pendant la phase de signalisation associée à l'établissement d'une liaison de communication à
10 travers un réseau de transmission. De plus, le procédé de l'invention permet de réduire les coûts de communication à travers le réseau de transmission.

L'invention propose en outre un dispositif d'émission-réception permettant de mettre en œuvre le procédé de l'invention.

L'invention a donc pour objet un procédé d'envoi d'un message
15 utilisateur à travers un réseau de transmission caractérisé en ce que :

- on active une demande d'établissement d'un canal de communication entre un appelant et un appelé,
- on réalise, pour l'établissement du canal de communication, une phase de signalisation pendant laquelle un message de signalisation,
20 comportant au moins un champ disponible, est échangé entre l'appelant et l'appelé,

et en ce que :

- on place, avant l'échange entre l'appelé et l'appelant, dans le champ disponible du message de signalisation le message utilisateur,
- 25 - on met fin à l'établissement du canal de communication une fois le message utilisateur, et ou une réponse au message utilisateur, reçu par l'appelé, et ou par l'appelant.

L'invention a également pour objet un dispositif d'émission et ou de réception d'un message utilisateur à un appelé à travers un réseau de
30 transmission caractérisé en ce qu'il comporte une mémoire dédiée, la mémoire dédiée ayant pour fonction de mémoriser le message utilisateur et ou la réponse au message utilisateur, ce message utilisateur et ou cette réponse étant envoyée dans un champ libre d'un message de signalisation pendant une phase de signalisation.

35 L'invention sera mieux comprise à la lecture de la description qui suit

et à l'examen des figures qui l'accompagnent. Celles-ci ne sont présentées qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent :

- Figure 1 : une architecture simplifiée d'un téléphone mobile permettant de mettre en œuvre le procédé de l'invention ;

5 - Figure 2 : une représentation, sous forme d'un algorithme, d'un exemple de fonctionnement du procédé de l'invention.

La figure 1 montre un exemple préféré d'application de l'invention. En effet, la figure 1 montre une architecture simplifiée d'un téléphone 1 mobile, mettant en œuvre le procédé de l'invention, relié à une station 2 de base d'un
10 réseau 3 de téléphonie mobile par une liaison 4 radioélectrique. Ainsi, le téléphone 1 est utilisé pour envoyer ou recevoir un message utilisateur, à travers un réseau de transmission tel que le réseau 3 par exemple. Pour assurer ces fonctions d'émission et de réception notamment, le téléphone 1 comporte une antenne 5 reliée à un dispositif 6 d'émission et de réception.
15 Ce dispositif 6 est contrôlé par un microprocesseur 7 commandé par un programme 8 dans une mémoire de programme 9 par l'intermédiaire d'un bus 10 de données, de commandes et d'adresses.

Dans cet exemple préféré, le téléphone 1 est utilisé, outre sa fonction de téléphonie mobile usuelle, comme interface de communication, ou encore
20 modem, entre un lecteur 11 d'une carte à puce 12 et un correspondant 13. Le lecteur 11 est, de manière préférée, placé dans le téléphone 1, mais pourrait très bien être seulement raccordé à ce dernier par une liaison filaire. Ainsi, le correspondant 13 est un centre d'authentification de la carte à puce 12. Le centre 13 est relié, directement par une liaison 14 où indirectement
25 par un réseau 15 de téléphonie fixe par exemple, à un circuit 16 de connexion du réseau 3. Ainsi, le téléphone 1 envoie au centre 13 un code secret de la carte 12 ainsi qu'un numéro d'identification, le code secret et le numéro d'identification étant placés dans un champ disponible du message de signalisation. L'ensemble composé du code secret et du numéro
30 d'identification est appelé par la suite identifiant.

Dans l'invention, on transmet le message utilisateur pendant une phase de signalisation associée à l'établissement d'une liaison de communication entre le téléphone 1 et le centre 13. En effet, on utilise pour cela un champ laissé disponible dans des messages de signalisation,
35 échangés entre le téléphone 1 et le dispositif 13, tel que décrit notamment

selon la norme GSM 04.08. Cette norme y définit de plus une procédure d'établissement d'une liaison de communication dans un réseau de téléphonie mobile, selon la norme GSM notamment.

Un champ disponible signifie qu'un message de signalisation est de longueur variable. Bien évidemment, lorsque le champ disponible n'est pas utilisé, on n'émet la partie correspondant à un champ donné que si celui-ci comporte une information. Un message de signalisation comporte ainsi différents champs, chacun relatif à un paramètre, dont un précise notamment une fonction associée à ce message. Il peut s'agir d'un message de commande ou d'un message de contrôle des différentes phases de signalisation nécessaires pour établir la liaison de communication.

Le code secret est produit à partir d'un clavier 17, par exemple du téléphone 1. Plus précisément, dans cet exemple préféré selon l'invention, lorsque la carte à puce 12 est insérée dans le lecteur 11 et qu'un code a été entré au clavier 17 alors le microprocesseur 7 active une demande d'établissement d'un canal de communication entre le téléphone 1 et le dispositif 13.

Selon une première caractéristique essentielle de l'invention le microprocesseur 7 utilise un des champs disponibles d'un message de signalisation, avant émission, pour y placer le message utilisateur. Dans l'invention, le message de commande qui est émis et qui comporte le message utilisateur, est un message spécial. Ce message spécial est un message de signalisation dont une valeur d'un paramètre permet d'indiquer à l'appelé lorsqu'il le reçoit, qu'un message se trouve dans le champ qui est normalement disponible. Pour réaliser cela, on peut utiliser une valeur prédéfinie qui indique que le protocole de communication est connu de l'appelant et de l'appelé. En conséquence, lorsque l'appelé reçoit un message de signalisation avec un tel paramètre alors il sait où se trouve le message utilisateur. Cependant, il est tout à fait envisageable de produire une nouvelle valeur en plus de celles prédéfinies et qui aboutirait au même résultat. Ainsi, le centre 13 émet à son tour un message de signalisation comportant cette fois-ci une réponse au message utilisateur, par exemple si l'authentification de la carte 12, en fonction de l'identifiant émis avec le message utilisateur, est positive ou négative.

Selon une deuxième caractéristique essentiel de l'invention, le

microprocesseur 7 met fin à l'établissement du canal de communication une fois le message 4, et ou une réponse au message 4, reçu par l'appelé ou par l'appelant. C'est à dire, si le téléphone 1 émet un message 4 et n'attend pas de réponse de la part du centre 13 alors ce dernier peut mettre fin à l'établissement du canal de communication. Si par contre une réponse est attendue par le téléphone 1, puisque dans cet exemple il est l'émetteur du message utilisateur, alors c'est celui-ci qui devra mettre fin à l'établissement du canal de communication. En effet, on considère dans ce document que la communication est totalement établie lorsque l'appelé accepte l'appel, c'est à dire, plus simplement, lorsqu'il décroche. Dans l'invention, l'appelé ne décroche pas mais reçoit tout de même le message utilisateur par l'intermédiaire des messages de signalisation. En conséquence, le coût d'une communication est nul puisque généralement il faut décrocher pour activer un compteur d'unité de paiement.

Dans une variante le dispositif 13 ou l'appelé pourrait être un autre téléphone 18 mobile, relié à une station 19 de base par exemple du réseau 3. Dans ce cas, le téléphone 1 et le téléphone 18 peuvent échanger des mini-messages tels que les messages utilisateurs. De plus, le téléphone 1 peut être relié à un ordinateur 20 utilisant ainsi le téléphone 1 comme modem. De même, le téléphone 18 peut être relié à un ordinateur 21.

Lorsqu'un modem, ici le téléphone 1, établit un canal de communication, alors celui-ci échange des messages de signalisation avec l'appelé, par exemple le téléphone 18, alors un message de signalisation est associé avec un registre, c'est à dire une zone mémoire. Ainsi, lorsque le programme 8 commande une émission du message utilisateur, il l'associe avec un premier message de signalisation et lorsque le téléphone 1 reçoit une réponse au message utilisateur alors celui-ci est associé avec un deuxième message de signalisation. Cette commande est associée avec une mémoire 22 dédiée qui fait office de registre. En conséquence, lorsque le téléphone 1 reçoit une réponse au message utilisateur, alors celle-ci est automatiquement mémorisée dans la mémoire 22, sur commande d'un sous programme de gestion associé au programme 8 en général. Le fonctionnement est le même du côté du centre 13 ou du téléphone 18, c'est à dire que lorsque le centre 13 ou le téléphone 18 reçoivent le message utilisateur alors celui-ci est mémorisé dans une mémoire dédiée (non

représenté) tel que la mémoire 22. Dans le cas des cartes à puces, le centre 13 mémorise ainsi dans une mémoire dédiée une valeur du code secret ainsi qu'une valeur d'un numéro de la carte à puce 12 et une valeur mémorisée dans le registre 22 pourrait correspondre à un acquittement positif ou négatif par le centre 13 selon que le code à été accepté ou refusé respectivement.

5 Dans un exemple préféré, on autorise un utilisateur à accéder à la mémoire 22 par l'intermédiaire de commandes spécifiques. Ainsi, cet utilisateur peut y placer des valeurs à émettre et ou y lire des valeurs reçues. Pour cela, il utilise notamment le clavier 17 du téléphone 1 ou le clavier de 10 l'ordinateur 20 si ce dernier est relié au téléphone 1. Dans un exemple, les commandes spécifiques sont des commandes de contrôle d'un modem. Cependant, un utilisateur pourrait, selon ses besoins, produire de nouvelles commandes spécifiques qui lui sont propres, on aurait alors des commandes dites propriétaires.

15 Dans une variante préférée de l'invention, on place la mémoire 22 dans le téléphone 1. Le fait d'utiliser une mémoire dédiée telle que la mémoire 22 permet d'avoir un fonctionnement plus souple du téléphone 1. En effet, on sait que lorsque l'on reçoit un tel message de signalisation alors il suffit d'effectuer une opération de lecture dans la mémoire dédiée associé, 20 avec le sous programme précédent, pour déterminer la valeur correspondante au message 4 reçu. Le fonctionnement du téléphone 13 ou du téléphone 18 est le même que pour le téléphone 1 en ce qui concerne l'utilisation d'une mémoire dédiée.

Dans une autre variante, on place la mémoire 22 dans un modem 25 (non représenté) de type RNIS. Ces modems permettraient de relier un appelant à un appelé par l'intermédiaire d'un réseau RNIS qui serait alors utilisé en tant que réseau de transmission de l'invention. Dans ce cas, en prenant l'exemple de l'ordinateur 20, celui-ci serait relié aux modems au lieu d'être relié au téléphone 1. Une phase de signalisation à travers un réseau 30 RNIS utilise des messages de signalisation comportant aussi, comme dans le cas du réseau 3 de téléphonie mobile, des champs disponibles.

Dans un exemple préféré de l'invention, la taille du message utilisateur est limitée à 35 octets au maximum. En effet, un champ disponible ne peut recevoir que des données dont une longueur binaire est inférieure à 35 35 octets.

La mémoire 22 a pour fonction de mémoriser le message utilisateur et ou la réponse au message utilisateur, ce message utilisateur et ou cette réponse sont à envoyer à l'aide d'un champ libre d'un message de signalisation. Ainsi, dans un exemple préféré, la mémoire 22 a une capacité
5 mémoire qui est au plus de 35 octets. Dans une autre variante, et pour permettre une transmission sécurisée du message utilisateur à travers le réseau 3 d'une part et à travers l'espace libre d'autre part, on chiffre avec une clé de chiffrage afin de le rendre incompréhensible pour un tiers. Lorsque le destinataire du message utilisateur reçoit ce message utilisateur
10 alors il utilise une clé de déchiffrement associé pour rendre compréhensible l'information portée par le message utilisateur.

La figure 2 montre, sous forme d'un algorithme, un exemple de fonctionnement du procédé de l'invention. On utilise comme exemple le cas de d'authentification d'un code secret de carte à puce tel que la carte à puce
15 12. On utilise pour cela comme dispositif d'émission réception le téléphone 1 de la figure 1 avec le lecteur 11. Ainsi dans une étape 23, on entre associé à la carte à puce 12 à l'aide du clavier 17. Avant cela, bien évidemment, le téléphone 1 a été configuré selon un fonctionnement spécial, c'est à dire qu'il fonctionne comme un lecteur de carte à puce. Une valeur de ce code secret
20 est mémorisée dans la mémoire 22 en attendant d'être émise.

Dans une étape 24 de mise en forme, le programme 8, ou plus précisément un sous programme de ce programme 8, commande le microprocesseur 7 pour envoyé le dispositif 6 d'émission réception la valeur mémorisée dans la mémoire 22 et ainsi de préparer le message utilisateur à
25 émettre. Ce message utilisateur comporte la valeur du code secret, chiffrée dans un exemple préféré, et est insérée dans un champ disponible d'un message de signalisation. Dans une étape 25, le message de signalisation comportant le message 4 était mis à destination du centre 13 d'authentification dans cet exemple. Dans une étape 26, le centre 13
30 procède à l'authentification, après déchiffrement du code secret ici reçu associé notamment à un numéro d'identification de la carte à puce 12. Une fois cette authentification terminée, le centre 13, dans une étape 27, transmet la réponse associée à cette authentification au téléphone 1.

Le téléphone reçoit ainsi, dans une étape 28, une réponse au
35 message utilisateur précédemment émit à l'étape 25 et mémorise la réponse

du centre 13 dans la mémoire 22. Un programme de traitement associé au fonctionnement du téléphone 1 en lecteur de carte à puces récupère dans la mémoire 22, lors d'une étape 29, un contenu de cette mémoire 22. Si le message d'authentification est positif en sortie d'une étape 30 de test alors le

5 microprocesseur 7 autorise, dans une étape 31, un paiement en informant pour cela un détenteur de la carte 12 par l'intermédiaire d'un message sonore et ou d'un message visuel. Dans le cas d'une authentification négative, l'autorisation, de l'étape 31, est refusée au détenteur de la carte à

10 puce 12. On réduit ainsi, avec l'invention, un temps d'accès au centre 13 et donc un temps de réponse, tout en limitant par la même un coût de communication à travers le réseau 3.

Cette description est basée sur un exemple concernant l'authentification d'un code à carte à puce mais il est évident que le procédé de l'invention peut être utilisé pour transmettre n'importe quel message de

15 quelques dizaine d'octets à un appelé. Ainsi, le domaine de l'invention concerne plus généralement la transmission de données à travers un réseau de transmission de type GSM ou RNIS.

REVENDICATIONS

1 - Procédé d'envoi d'un message utilisateur à travers un réseau (3) de transmission caractérisé en ce que :

5 - on active une demande d'établissement d'un canal de communication entre un appelant et un appelé,

 - on réalise, pour l'établissement du canal de communication, une phase de signalisation pendant laquelle un message de signalisation, comportant au moins un champ disponible, est échangé entre l'appelant et
10 l'appelé,

 et en ce que :

 - on place, avant l'échange entre l'appelé et l'appelant, dans le champ disponible du message de signalisation le message utilisateur,

 - on met fin à l'établissement du canal de communication une fois le
15 message utilisateur, et ou une réponse au message utilisateur, reçu par l'appelé et ou par l'appelant.

2 - Procédé selon la revendication 1 caractérisé en ce que :

 - on mémorise le message utilisateur et ou une réponse au message utilisateur dans une mémoire (22) dédiée du récepteur du message
20 utilisateur et ou de la réponse au message utilisateur respectivement.

3 - Procédé selon la revendication 2 caractérisé en ce que :

 - on autorise un utilisateur à accéder à la mémoire dédiée par l'intermédiaire de commandes spécifiques.

4 - Procédé selon l'une des revendications 1 à 3 caractérisé en ce
25 que:

 - on place la mémoire dédiée dans un téléphone (1) mobile, le téléphone mobile étant utilisé comme modem, le réseau de transmission étant alors un réseau de téléphonie mobile.

5 - Procédé selon l'une des revendications 1 à 3 caractérisé en ce
30 que:

 - on place la mémoire dédiée dans un modem de type RNIS, le modem permettant de relier l'appelant à l'appelé par l'intermédiaire d'un réseau RNIS utilisé en tant que réseau de transmission.

6 - Procédé selon l'une des revendications 1 à 5 caractérisé en ce
35 que:

10

- on limite la taille d'un message utilisateur à 35 octets maximum.

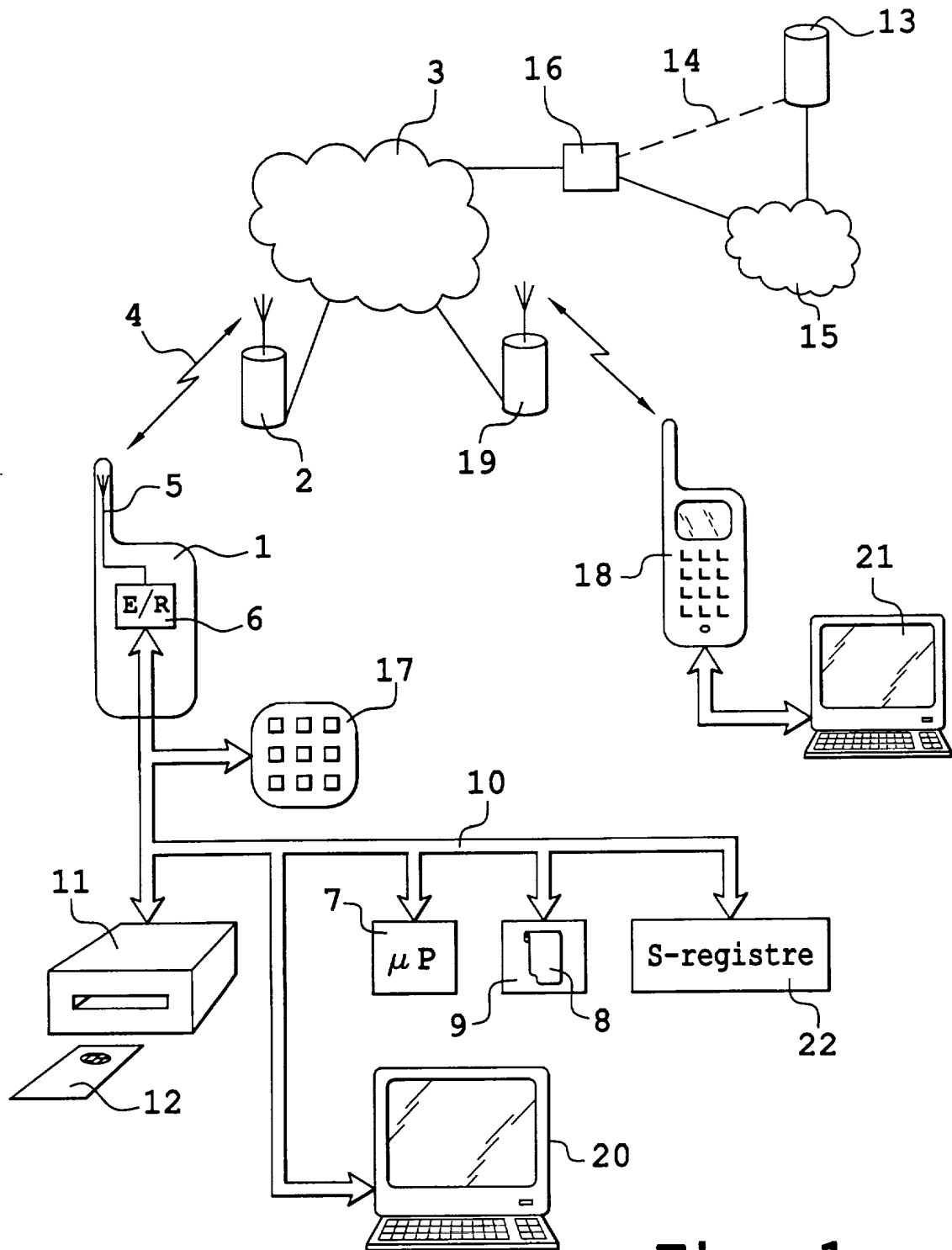
7 - Procédé selon l'une des revendications 1 à 6 caractérisé en ce que:

- 5 - on chiffre, avec une clé de chiffage, le message utilisateur avant émission,
- on déchiffre, avec une clé de déchiffage, le message utilisateur à la réception.

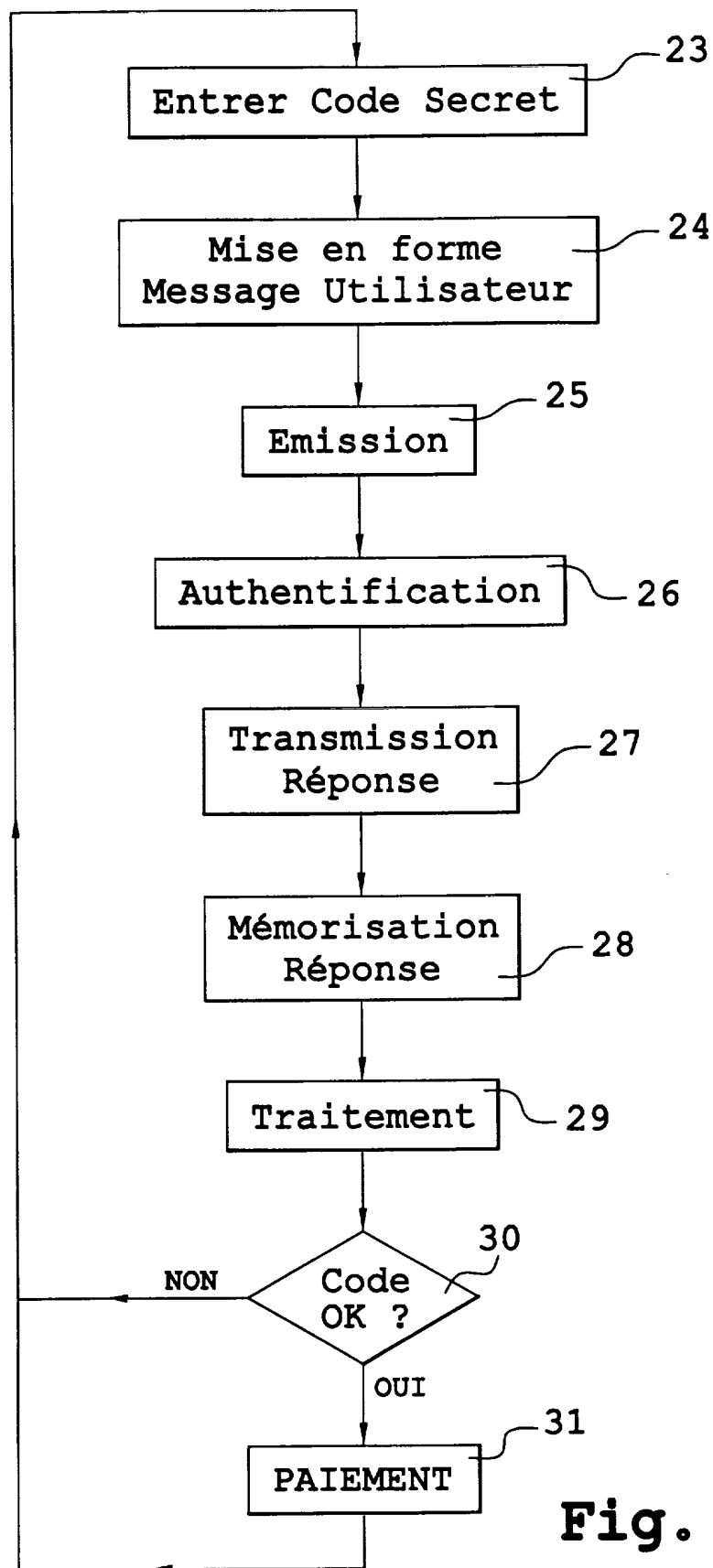
8 - Dispositif (1) d'émission et ou de réception d'un message utilisateur à un appelé à travers un réseau de transmission caractérisé en ce qu'il
10 comporte une mémoire (22) dédiée, la mémoire dédiée ayant pour fonction de mémoriser le message utilisateur et ou la réponse au message utilisateur, ce message utilisateur et ou cette réponse étant envoyée dans un champ libre d'un message de signalisation pendant une phase de signalisation.

9 - Dispositif selon la revendication 8 caractérisé en ce qu'une
15 capacité mémoire de la mémoire dédiée est au plus de 35 octets.

1/2

**Fig. 1**

2/2

**Fig. 2**

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

2802743

N° d'enregistrement
national

FA 584034
FR 9916050

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
E	EP 1 009 153 A (SAGEM) 14 juin 2000 (2000-06-14) * abrégé * * page 2, colonne 1, ligne 47 - ligne 55 * * page 2, colonne 2, ligne 16 - ligne 22 * * page 2, colonne 2, ligne 36 - page 3, colonne 3, ligne 54 * ---	1-9	H04L12/58 H04Q7/20
E	WO 00 24225 A (QUALCOMM INC) 27 avril 2000 (2000-04-27) * abrégé * * page 2, ligne 16 - page 3, ligne 16 * * page 6, ligne 1 - ligne 15; revendication 1 * ---	1-9	
X	GLITHO R H: "USE OF SS7 IN D-AMPS-BASED PCS: ORTHODOXY VS. HETERODOXY" IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 4, no. 3, 1 juin 1997 (1997-06-01), pages 15-23, XP000655312 ISSN: 1070-9916 * abrégé * * page 17, colonne de gauche, ligne 38 - colonne de droite, ligne 14 * * page 19, colonne de droite, ligne 11 - page 20, colonne de droite, ligne 22 * -----	1-9	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04Q
Date d'achèvement de la recherche		Examineur	
1 décembre 2000		Adkhis, F	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire 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 & : membre de la même famille, document correspondant			