(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 817 144 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
07.01.1998 Bulletin 1998/02

(51) Int Cl.[6]: **G08B 5/22**

(21) Numéro de dépôt: **97401610.7**

(22) Date de dépôt: **04.07.1997**

(84) Etats contractants désignés:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priorité: **05.07.1996 MX 9600261**
31.10.1996 FR 9613370

(71) Demandeur: **GEMPLUS**
13420 Gemenos (FR)

(72) Inventeurs:
- **Lezama Argaez, Hector Alberto**
  75116 Paris (FR)
- **Leduc, Michel**
  75116 Paris (FR)
- **Karlisch, Thierry**
  75116 Paris (FR)

(74) Mandataire: **Schmit, Christian Norbert Marie et al**
Cabinet Ballot-Schmit
7, rue Le Sueur
75116 Paris (FR)

(54) Procédé de contrôle de l'utilisation d'un messageur, messageur fonctionnant selon ce procédé et carte à puce pour l'accès conditionné à un messageur

(57) Pour contrôler l'utilisation d'un messageur (1) on prévoit d'associer à ce messageur une carte (21) à puce (25) . Au moment de la délivrance d'un message, on décompte des unités dans une mémoire (26) d'unités prépayées de la carte à puce, de façon à permettre une gestion du service de messagerie proportionnelle à l'utilisation. En variante, la carte à puce possède un circuit (PIN, 27) d'authentification qui permet de vérifier que le porteur de la carte à puce est habilité à recevoir tout ou partie des messages contenus dans le messageur.

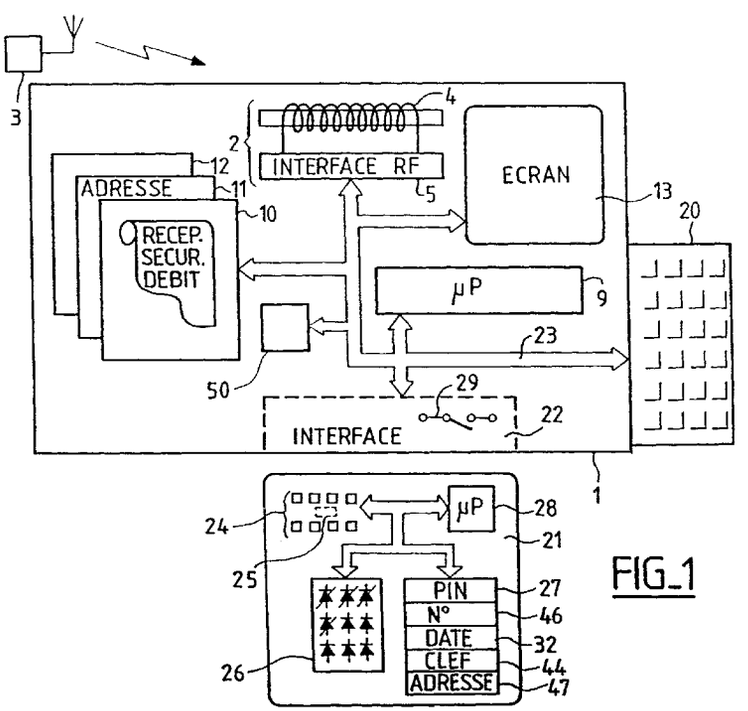


FIG_1

EP 0 817 144 A1

Description

La présente invention a pour objet un procédé de contrôle de l'utilisation d'un messageur, dit "pager" ou "pageur" dans le langage commun. L'invention a pour objet de rationaliser l'utilisation de tels dispositifs. Elle concerne également un messageur fonctionnant selon ce procédé et une carte à puce pour conditionner l'accès à ce messageur.

Un messageur est un appareil de réception, quelques fois de réémission, qu'un utilisateur porte généralement sur lui et qui lui permet d'être alerté par un correspondant sur une action à entreprendre où une information à connaître. Dans le cas général, la transmission entre l'émetteur d'un message et le messageur est effectuée par voie hertzienne. Cependant, il est tout à fait possible que cette transmission se fasse par voie filaire ou autres: par exemple en connectant régulièrement le messageur auprès d'une borne d'un ensemble de bornes disséminées sur un territoire et en recevant les messages qui sont stockés en attente et qui lui sont destinés.

Les communications personnelles mobiles par l'intermédiaire de récepteurs radio sont populaires depuis quelques années, notamment les récepteurs radio recevant des messages texte transcrits sur des écrans à cristaux liquides. Dans les appareils de communication personnelle mobiles ou de table, on peut citer également les téléphones cellulaires.

L'objet de la présente invention est d'incorporer une carte à puce aux récepteurs déjà opérationnels.

L'utilisation de cartes de contrôle est devenue également habituelle pour différentes sortes d'appareils, par exemple, pour des téléphones publics à carte. Les cartes de crédit font également partie des antécédents de l'invention.

Dans le cas où l'émission du message est effectuée par voie radio-électrique, le message est émis par un opérateur au moyen d'un codage d'une porteuse en modulation de fréquence. L'émetteur envoie cycliquement les messages des différents interlocuteurs concernés de façon à être sûr que ceux-ci les ont bien reçus. Le messageur comporte un récepteur d'ondes radio-électriques avec un code d'identification personnel. Le récepteur est capable de détecter les messages émis et de choisir parmi les messages émis ceux qui lui sont destinés. Au moment de la réception d'un tel message, le messageur produit une alarme, une émission sonore, une vibration, ou un affichage lumineux sur un afficheur. En général sur l'afficheur du messageur appelé on peut même lire le numéro de l'appelant, éventuellement directement le message de l'appelant. Dans certains systèmes, l'appelé peut envoyer un accusé de réception grâce à son messageur. Généralement il rappelle au moyen d'un téléphone le plus proche l'interlocuteur qui cherche à le joindre.

Un tel service était jusqu'à présent réservé aux professionnels. Mais on voit récemment une évolution vers des applications grand public avec l'arrivée de messageurs à bas coût. La modification de la clientèle appelle par ailleurs une mise en place de nouveaux services.

Aujourd'hui les systèmes de radio-messagerie fonctionnent soit par abonnement, soit par la rémunération de l'opérateur d'émission au travers de l'appel téléphonique de l'appelant, et de celui, en réponse de l'appelé. Le défaut du système actuel de rémunération de l'opérateur réside dans le fait que l'appelé peut utiliser un autre réseau que celui de l'opérateur pour rappeler. Même parfois, il ne rappelle pas dans la mesure où le message est suffisamment significatif pour éviter l'appel.

Bien qu'un tel système soit un moyen particulièrement efficace pour pallier un manque de réseaux téléphoniques et/ou peu de postes chez l'habitant, il a l'inconvénient d'être onéreux à l'achat et/ou avec une formule d'abonnement. Dans certains cas, des utilisateurs vont jusqu'à utiliser le service de télécommunication sans payer leur abonnement.

En outre, au moment où on envoie un message avec un tel système à un destinataire, il convient de s'assurer que le porteur du messageur est bel et bien la personne à qui était destiné le message et non pas une personne étrangère, ou éventuellement un fraudeur. Ceci pourrait être gênant si un étranger était informé du contenu du message qui ne lui serait pas destiné. De préférence on cherche à régler les deux problèmes en même temps. L'objectif de l'invention est de permettre l'équipement, en particulier des abonnés, en ayant l'assurance qu'ils s'acquittent du service de télécommunication qui leur est proposé.

La solution de ces problèmes est obtenue avec un messageur selon l'invention qui permet de le donner ou de le vendre à un utilisateur. On récupère alors l'investissement et/ou le service proposé par l'opérateur en faisant payer l'utilisateur, de préférence chaque fois qu'un message lui est délivré, de manière obligatoire, sans fraude ou échappatoire possible. Dans ce but, on munit chaque messageur dans un exemple d'un support électronique portable: dans la pratique une carte à puce. Le messageur comporte alors un lecteur de carte à puce et n'est autorisé à fonctionner que si une carte à puce adéquate est engagée dans le messageur. Dans un cas, la carte à puce sera une carte à puce du type avec unités prépayées de telle sorte qu'il sera possible d'y décompter des unités au fur et à mesure de la réception des messages, et de n'autoriser leur délivrance au porteur du messageur que si le nombre d'unités disponibles a été suffisant. Dans ce cas, on résoudra par ailleurs plus facilement l'adéquation du porteur du messageur au destinataire du message en identifiant et/ou en authentifiant le porteur par le biais de la carte à puce engagée dans le messageur. De cette façon, on pourra même prévoir un messageur susceptible de recevoir et de mémoriser des messages destinés à plusieurs destinataires et ne permettant la délivrance des messages d'un destinataire que si ce destinataire a engagé sa propre

carte à puce dans le messageur. On peut alors réaliser un sous-adressage qui soit fonction d'une adresse contenue dans le messageur et d'une sous adresse contenue dans la carte. Grâce à cette fonction multi-utilisateurs, il est possible de partager les frais d'acquisition d'un messageur entre plusieurs personnes. Dans ce cas, le messageur peut fonctionner éventuellement en poste fixe accessible à chaque utilisateur. Dans un autre exemple, le messageur effectue tout seul toutes ces fonctions sans adjonction de carte.

Dans le cas multi-utilisateurs, l'identification du destinataire s'effectue par le biais d'un code dit PIN que chaque destinataire introduit sur un clavier prévu à cet effet sur le messageur. Les moyens permettant de réaliser la fonction ci-dessus (multi-utilisateurs) sont de type connus.

La présente invention incorpore une carte à puce de contrôle, ou carte intelligente, à un récepteur radio de messages texte, transcrits sur des écrans à cristaux liquides, ci-après le messageur, carte qui réalise plusieurs fonctions de la façon suivante :

- un récepteur personnel, une fois allumé, reste en attente de réception des messages; à chaque message, un signal apparaît à l'écran (écran à cristaux liquides);
- lorsque l'utilisateur du récepteur perçoit le signal, il insère une carte à puce afin d'obtenir chacun des messages à l'écran.
- la carte est de préférence une carte prépayée qui ne fera fonctionner le récepteur que si elle a le crédit suffisant pour que le message soit reproduit; c'est-à-dire que la fonction de la carte est de donner accès au message à l'écran, ce qui sous-entend que la délivrance du message est conditionné à l'insertion de la carte à puce;
- la carte à puce peut par ailleurs être conçue pour réaliser une fonction de déchiffrage permettant à chaque message d'être reproduit, la fonction de la carte étant de déchiffrer un message, ce qui sous-entend que la carte traduit le signal, par l'intermédiaire d'un code, en un texte dans un langage connu, chaque message représentant un coût qui est déduit de la valeur de la carte.

Par conséquent, la carte à puce faisant l'objet de la présente invention, dans une première réalisation, a pour fonction la régulation du prépaiement des messages transcrits en texte sur l'écran à cristaux liquides, ce qui contrôle un certain nombre de messages ainsi que la dimension de ces derniers.

Dans une seconde réalisation, la carte à puce faisant l'objet de la présente invention comprend, outre les fonctions ci-dessus, le déchiffrage de chaque message qu'elle traduit par l'intermédiaire d'un code vers un texte en langage connu.

Il y a plusieurs façons de réaliser la présente invention sans pour autant sortir de son cadre puisqu'il faut la considérer dans son sens le plus large et non limitatif.

L'invention a donc pour objet un procédé de contrôle de l'utilisation d'un messageur comportant les étapes suivantes:

- le messageur reçoit des messages envoyés par un émetteur,
- on vérifie que les messages reçus sont destinés au messageur, et quand c'est le cas on les mémorise dans le messageur,
- puis on les délivre au porteur du messageur,

caractérisé en ce que, avant de les délivrer,

- on vérifie en plus que le porteur du messageur est autorisé à connaître ce qui est diffusé.

L'invention a également pour objet un messageur comportant un circuit de réception de message et un circuit de délivrance des messages reçus, caractérisé en ce qu'il comporte un lecteur de support à puce, carte à puce, un support à puce engagé dans le lecteur, et un circuit pour autoriser la délivrance des messages reçus lorsqu'un support à puce correct est engagé dans le lecteur.

L'invention a aussi pour objet une carte à puce pour récepteur radio de messages transcrits en texte sur écran à cristaux liquides, caractérisée en ce qu'un récepteur est équipé des éléments pour recevoir la carte, laquelle carte contrôlera le crédit qui ne fera fonctionner le récepteur que si le solde est suffisant pour reproduire le message, c'est-à-dire que la fonction de la carte est de donner accès au message à l'écran, ce qui sous-entend que le message est conditionné à l'insertion de la carte.

Pour cela, l'invention a pour objet un messageur dont le fonctionnement et/ou la délivrance du message est subordonné de préférence à un paiement d'unités prépayées contenues dans une mémoire.

Selon un premier mode de réalisation, les unités sont contenues dans une mémoire d'une carte à puce, le messageur coopérant avec ladite carte pour débiter lesdites unités.

Selon un deuxième mode de réalisation, les unités sont contenues dans une mémoire du messageur, celui-ci fonctionnant de manière autonome pour les débiter.

Dans les deux cas, il y a deux variantes envisageables:

- à unités non rechargeables, (le messageur ou la carte étant jetable);
- à unités rechargeables. Les unités sont de préférence rechargeables par tous moyens de chargement notamment à distance (radio-électrique, avec des cartes à puce sans contact ou par utilisation du messageur lui-même, infrarouge, électro-acoustique).

L'avantage est alors de réutiliser les mémoires et d'éviter de se déplacer pour acheter des cartes à puces.

L'invention a enfin pour objet une carte à puce pour récepteur radio de messages transcrits en texte sur écran à cristaux liquides, caractérisée en ce qu'elle réalise la fonction de déchiffrage permettant de reproduire chaque message, c'est-à-dire qu'elle déchiffre un message par l'intermédiaire d'un code qui traduit le signal en un texte en langage connu.

Selon une autre caractéristique de l'invention, le messageur réalise une fonction sécuritaire du chargement des unités. La sécurité s'effectue soit dans le messageur, de préférence à l'aide d'un module de sécurité applicatif, soit dans une carte à microprocesseur. Un module de sécurité applicatif est inaccessible et inviolable du fait d'une protection physique de ce composant. La protection peut être passive ou active. Un tel module met typiquement en oeuvre un protocole de reconnaissance et d'agrément du type de ceux connus dans le domaine des cartes à puce.

Les étapes du rechargement sont les suivantes. L'utilisateur va chez un distributeur pour faire recharger un messageur ou sa carte. Il donne le numéro d'identité du messageur ou de la carte et l'argent correspondant à l'achat d'unités. Le distributeur appelle un serveur central qui envoie un signal de rechargement comportant le numéro d'identité qui a été transmis préalablement, et éventuellement un code représentatif d'un code secret. Le microprocesseur du messageur ou de la carte effectue un test de comparaison entre le code du message et celui contenu dans le module de sécurité applicatif (ou dans la carte) avant d'incrémenter la mémoire d'unités d'un nombre d'unités convenu.

En alternative, la commande d'un chargement d'unités et le paiement peuvent être effectués directement par correspondance.

Pour des raisons pratiques de simplicité, le signal de rechargement est de préférence émis de la même manière que pour l'émission des messages.

Pour des raisons de sécurité, le signal de rechargement peut être émis sur une borne déterminée, pour centraliser le chargement et éviter qu'un autre messageur puisse capter le signal de rechargement. La borne peut être contenue dans une cabine, ou un poste, de téléphone par exemple, ou être une borne infrarouge.

Dans le cas d'une cabine ou d'un poste de téléphone, l'utilisateur peut lui-même communiquer les données ci-dessus au serveur central par la ligne téléphonique, et recevoir le chargement par la ligne. Des moyens de réception de signaux acoustiques, notamment du type DTMF, peuvent être prévus dans le messageur. De tels moyens sont connus de l'homme de l'art.

Pour éviter la fraude consistant notamment en une dérivation du signal à la sortie de l'antenne de réception, le message peut être crypté à l'émission, puis stocké, avant délivrance, dans une mémoire quelconque du messageur ou dans la carte. Le message est ensuite délivré après une étape de décryptage réalisée par un module de sécurité applicatif. Le module de sécurité applicatif comporte dans ce cas au moins un microprocesseur et un algorithme de décryptage. Le message peut également être stocké directement dans une zone mémoire du module de sécurité applicatif. La fonction de gestion du messageur et celle du microprocesseur de la carte peuvent être réalisées par un seul microprocesseur contenu dans un tel module de sécurité applicatif.

Le module de sécurité applicatif est de préférence compris dans le messageur. Dans une variante du premier mode, le module de sécurité applicatif peut être compris dans la carte, qui réalise ainsi elle-même tout ou partie de la fonction de décryptage.

Dans le cas du premier mode, pour éviter une fraude par l'usage de fausse carte, le messageur est apte à réaliser une procédure d'authentification de la carte. On peut utiliser avantageusement une carte à mémoire bas de gamme de type carte téléphonique (télécarte) dite de première génération réalisant simplement une fonction de stockage d'unités, d'identification et d'authentification passive (sans microprocesseur). Mais il est préféré une carte dite de deuxième génération (toujours sans microprocesseur) permettant de réaliser une procédure d'authentification active de celle-ci et éventuellement du messageur.

Ainsi, le messageur fonctionne avec un degré de sécurité raisonnable, avec des cartes téléphoniques standards bon marché, dont l'acquisition est accessible par les personnes visées précédemment.

Le messageur peut réaliser une procédure d'authentification et/ou d'identification du destinataire. L'authentification est réalisée par exemple par l'introduction d'un code secret dans le messageur sur demande de celui-ci. Ce code secret peut également servir à débiter une carte de type bancaire.

Dans le cas d'un messageur multi-utilisateurs, l'identification du destinataire peut être effectuée par l'intermédiaire d'un code d'identification contenu dans la carte. Ces deux dernières fonctions relatives à l'identification et à l'authentification peuvent être cumulées.

Le module de sécurité est avantageusement utilisé pour plusieurs fonctions du messageur, notamment pour accueillir tout ou partie d'un circuit pour autoriser la délivrance des messages reçus, mais également tout ou partie d'un algorithme de décryptage, et/ou tout ou partie d'un circuit apte à réaliser un rechargement d'une mémoire en unités prépayées.

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 données qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent:

- Figure 1: Un messageur conforme à l'invention;
- Figure 2: les étapes principales du procédé de contrôle d'utilisation d'un messageur selon l'invention;
- Figure 3: la structure type d'un message envoyé par un émetteur à un messageur dans l'invention;

- Figure 4: la structure type d'un message enregistré dans la mémoire du messageur et susceptible d'être diffusé par ce messageur;
- Figure 5: un récepteur radio, modèle de table, commandé par une carte intelligent selon l'invention;
- Figure 6: le même récepteur en version portable.

La figure 1 montre un messageur dans lequel il va être possible de mettre en oeuvre le procédé de contrôle de l'invention. Ce messageur comporte un boîtier 1 muni d'un circuit de réception 2, pour recevoir des messages envoyés par un émetteur 3. Dans l'exemple représenté, l'émetteur 3 est un émetteur radio-électrique mais ce pourrait être aussi bien une banque de données reliée à des bornes auxquelles on pourrait en cas de besoin connecter le messageur 1. Dans un exemple le récepteur 2 comporte une bobine radio-fréquence 4 reliée à un circuit électronique d'interface radio-fréquence 5. Le circuit de réception 2 assure, en particulier dans le cas de l'émission radio-électrique, la réception, la détection, des informations et l'amplification du signal radio-électrique reçu au cours des étapes initiales 6 et 7 du procédé (figure 2). L'interface 5 effectue également, dans le cas de l'émission radio-fréquence, la démodulation du signal électrique reçu au cours d'une étape 8. L'opération de démodulation comportera naturellement une étape de numérisation pour que toute la suite du traitement du message reçu puisse être effectuée en binaire. Si la transmission n'est pas radio-électrique les étapes 6 à 8 peuvent être absentes.

Dans l'état de la technique, le messageur comporte un circuit câblé où un microprocesseur 9 qui gère toutes ses opérations. Le micro-processeur 9 est en relation par un bus 23 de données, d'adresses et de commandes avec une mémoire programme 10, des mémoires de données 11 et 12 et un afficheur 13. Dans un exemple l'afficheur 13 est un écran à cristaux liquides. Le microprocesseur 9 effectue au moment de la réception une vérification de ce que le message reçu dans le messageur est bien destiné au messageur. Dans ce but le message, figure 3, comporte deux éléments principaux d'une part l'adresse du messageur 14 et d'autre part le contenu 15 du message. Le micro-processeur 9 prélève alors dans une mémoire 11 de paramétrisation du messageur une information relative à l'adresse de celui-ci.

Dans l'invention cette information peut être gardée secrète et protégée par exemple dans un bloc de sécurité. Cette sécurité est également préférée notamment pour assurer le rechargement en unités prépayées dans une mémoire du messageur et/ou de la carte.

Au cours d'une opération 16 de vérification de destination, le micro-processeur 9 vérifie que l'adresse en mémoire 11 est la même que l'adresse dans la partie 14 du message. En cas de succès au cours d'une opération 17, le micro-processeur 9 provoque l'enregistrement du message reçu dans la mémoire 12. Les mémoires 10, 11, 12 peuvent par ailleurs être réunies en une seule qui comporterait des zones correspondantes. Les mémoires 10 et 11 de type non volatiles sont de préférence non effaçables, la mémoire non volatile 12 est de préférence effaçable et reprogrammable.

D'une manière classique, le micro-processeur 9 en mettant en oeuvre le sous-programme de réception contenu dans la mémoire 10 pourra provoquer l'émission d'une alarme consécutive ou simultanée à la mémorisation. Le micro-processeur 9 peut également afficher en permanence, ou après l'alarme, un menu 19, invitant le porteur de messageur à notamment faire apparaître son message. Dans ce but le messageur de l'état de la technique comporte de plus un clavier 20 en relation avec le micro-processeur 9 pour permettre au porteur de commander le messageur et de faire délivrer le message. Les étapes 18 et 19 peuvent ne pas exister, le porteur consultant régulièrement son message pour savoir s'il a reçu des messages.

Dans l'invention, pour résoudre les problèmes indiqués, on a eu l'idée, dans un exemple, de mettre le messageur 1 en relation avec un support à puce, de préférence une carte à puce 21. Dans ce but, le messageur comporte une interface 22 reliée au bus 23, de données d'adresses et de commande du messageur 1. Dans un exemple, l'interface 22 comporte un connecteur pour entrer en relation avec des plots 24 de connexion de la puce 25 du support 21. La liaison fonctionnelle du support à puce avec le messageur 1 peut aussi être hertzienne dans le cas d'une carte à puce sans contact. Selon l'invention, la puce 25 comportera au moins une des deux mémoires suivantes: une mémoire d'unités prépayées 26 et une mémoire de paramètres 27. De préférence, elle les comportera toutes les deux. De préférence également, elle comportera un micro-processeur 28. Le micro-processeur 28 n'est pas nécessaire si le micro-processeur 9, pour un mode de fonctionnement donné est autorisé à prendre la main sur les mémoires 26 et 27. Ceci est généralement le cas pour les cartes à puce téléphoniques standards.

Dans un exemple, l'insertion d'un support à puce 21 dans l'interface 22 sera détecté, par exemple par un contact de type fin de course 29 monté dans cet interface 22. Cette détection permet d'envoyer un ordre par le bus 23 au micro-processeur 9 pour que celui-ci lance un programme SECUR. de vérification, de ce que le porteur du messageur est autorisé à connaître et qui doit être délivré. Ainsi après une opération 30 de vérification de la présence du support, le micro-processeur 9, assisté au besoin du micro-processeur 28, va vérifier d'une part que la carte à puce introduite est une carte apte à fonctionner avec le messageur 1 et/ou par un programme DEBIT que la puce 25 comporte dans sa mémoire 26 suffisamment d'unités prépayées encore disponibles pour autoriser la délivrance du message qui a été reçu et mémorisé. Quand le microprocesseur 28 assiste, ou plutôt prend le relais du microprocesseur 9, c'est parce que la puce 25 comporte une mémoire programme (non représentée) reliée à ce microprocesseur 28 comme la mémoire 10 est reliée au microprocesseur

9.

Les deux étapes d'authentification de la carte à puce et de débit d'unité peuvent être mise en oeuvre isolément ou ensemble quel que soit leur ordre selon un mode de vérification retenu préalablement.

Ainsi, si on se contente de vérifier par un numéro d'identification personnelle (PIN) que le porteur du messageur et de la carte à puce est autorisé à l'utiliser, cela revient à avoir organisé un abonnement de type permanent. Plutôt que de seulement vérifier la composition d'un code porteur PIN, à la place, on peut au cours de l'opération 31 d'authentification de la carte vérifier qu'une date de validation 32, mémorisée dans la mémoire 27 est postérieure à une date 33 contenue dans une partie supplémentaire 34 de signalisation du message (figure 3). Dans ce cas on réalise un abonnement en temps limité.

Il est possible de munir le messageur d'un module 50 de sécurité applicatif. Celui-ci est aussi relié au bus 23. Il permet notamment de mettre en oeuvre, pour le messageur 1, un protocole d'authentification du porteur du messageur. Dans ce cas celui-ci peut fonctionner sans carte à puce, les fonctions de celle-ci étant toutes assurées par ce module du messageur.

Dans l'autre cas, au cours d'une opération 35 on vérifie le contenu d'unités disponibles dans la mémoire 26, et on oblitère celles de ces unités disponibles qui sont nécessaires pour permettre la délivrance du message. Le décompte de ces unités peut être arbitraire: par exemple une unité par message. Il peut être lié à la longueur de la partie 15 du message: à la longueur du contenu. Le nombre de ces unités peut également être imposé par un indice de consommation 350 présent en zone 34 du message. Par cet indice, l'opérateur de télécommunication qui gère l'émetteur 3 peut pondérer le coût de l'envoi du message, en fonction ici encore une fois de la longueur du message, ou en fonction de l'instant où le message est diffusé: heures creuses, heures pleines, ou même encore en fonction du caractère national ou international des émissions par les émetteurs 3 du même message, compte tenu du fait que le porteur du messageur peut successivement se trouver dans une ou plusieurs régions du monde. Il peut aussi être lié à un profil d'utilisateur, l'accès à certains messages (groupés par exemple) étant subordonné à la présence d'un profil contenu dans la carte. Le montant à payer peut éventuellement être dépendant de ce profil.

L'opération 31 d'authentification mise en oeuvre par le micro-processeur 9 conjointement avec le micro-processeur 28 est de type classique. Elle comporte la comparaison d'un code frappé avec le clavier 20 par le porteur du messageur et de la carte à puce 21 avec un code (secret ou non) PIN enregistré dans la mémoire 27. Ces opérations de vérification peuvent subir par ailleurs d'une manière connue des opérations de chiffrement pour empêcher que le code PIN mémorisé dans le support 21 puisse à la longue être découvert.

Les opérations de décompte d'unités sont elles aussi de type classique. La mémoire 26 est par exemple une mémoire comprenant des cellules mémoires de type non-volatile, uniquement programmables: leur passage d'un état vierge ou effacé à un état programmé étant équivalent à une consommation d'unités. Les unités peuvent également être constituées par la présence de fusibles qui sont claqués successivement. Eventuellement, la mémoire 26 est du type effaçable et programmable. Dans ce cas, le support 21 peut être rapporté comme indiqué précédemment auprès des services de l'opérateur qui gère l'émetteur 3 pour que celui-ci les recharge, contre un paiement bien entendu. A cette occasion, dans le cas où on a retenu une formule avec abonnement, il est possible que la date 32 enregistrée dans la mémoire 27 soit elle aussi reprogrammée de sorte que cette mémoire, au moins pour cette partie, serait de type effaçable et programmable. Elle comporterait de préférence dans ce cas des cellules mémoires de type EEPROM.

La mémoire 12 du messageur comporte des enregistrements des messages reçus et mémorisés à l'étape 17. Chaque enregistrement comporte, dans cette mémoire 12 un numéro d'ordre 36, éventuellement une description sommaire 37, permettant au porteur du messageur de se faire une idée du message enregistré. Chaque enregistrement comporte encore une zone 38 relative au message proprement dit et une zone 39 utilisable dans le cas où des unités ont dû être décomptées pour permettre la délivrance du message. La zone 39 peut comporter elle-même deux sous-zones, une première sous-zone 40, optionnelle, de débit dans laquelle figure le nombre d'unités qu'il faudrait payer pour pouvoir voir le message, et une zone 41 dans laquelle figure le nombre des unités déjà payées pour permettre la délivrance du message. La zone 41 peut ne contenir qu'un seul bit indiquant selon son état que la carte 21 a déjà été débitée dans sa zone 26 ou qu'elle ne l'a pas été.

Au moment de l'opération de débit, dans le cas où la consommation n'est pas unitaire mais est fonction soit du contenu du message soit de l'indice 350, on prélèvera dans la mémoire 26, des unités pour les inscrire dans la zone 41 jusqu'à concurrence du montant indiqué dans la zone 40. On peut de ce fait facilement compléter les unités déjà prélevées dans une carte 21 par des unités prélevées sur une carte 21 suivante, dans le cas où le contenu de la première n'aurait pas été suffisant. L'opération DEBIT de débit enregistrée dans la mémoire programme 10 du messageur 1 consiste donc à lire le contenu de la zone 40 (s'il y en a un), à lire le contenu de la zone 41, et à prélever à titre d'unités dans la mémoire 26 la différence de ces deux contenus. De cette façon un seul type d'instructions DEBIT peut servir pour les mises à jour.

Au moment où l'opération 35 de débit d'unités a été effectuée, il reste à aller relire la mémoire 12 au cours d'une opération 42. Cette opération 42 effectuée par le micro-processeur 9 n'est bien entendu lancée que dans la mesure où les opérations 30, 31 et 35 préalable ont

été couronnées de succès (toutes ou l'une d'entre elles seulement selon le mode opératoire retenu). Au moment de la lecture, il est possible que le contenu du message enregistré dans la zone 38 soit un message chiffré. Dans ce cas on peut avec le micro-processeur 9, ou éventuellement le micro-processeur 28, provoquer le déchiffrement 43 de ce message à l'aide d'une clé qui est contenue dans une zone 44 de la mémoire 27. En fin de compte, au cours d'une étape 45, le message est diffusé. La délivrance la plus simple consiste à afficher le message sur l'écran 13. Néanmoins, il est possible, si le messageur 1 comporte un haut parleur et des circuits de conversion d'un message écrit en un message de parole, de délivrer oralement le message mémorisé.

Avec les options du menu 19, il pourra dans l'invention être sélectionné n'importe quel message préalablement enregistré et ce message pourra être diffusé autant de fois qu'on le désire sous réserve, soit que la carte à puce 21 d'authentification ait été engagée dans le messageur 1 si l'authentification est requise, soit qu'en zone 41 une indication mentionnant le décompte d'unités soit présente, soit les deux conditions réunies en même temps. De préférence, le déchiffrage du message sera toujours effectué à la fin, de manière à ne stocker qu'une information chiffrée dans la zone 38. Dans ce cas la présence de la carte sera de préférence nécessaire pour y prélever la clef 44.

Dans le cas où le messageur peut être un messageur correspondant à plusieurs destinataires, il est possible d'utiliser à titre de complément d'adresse des informations mémorisées dans la mémoire 27 de la carte à puce, par exemple, le numéro de série 46 de celle-ci ou même une adresse 47. Dans ce cas, l'adresse messageur contenue dans la zone 14 du message est plus longue que l'adresse utile (celle qui permet de discriminer les différents messageurs). Elle comporte un complément d'adresse 48.

Dans ce cas, le messageur 1 reçoit les messages destinés à plusieurs destinataires. Les compléments d'adresse 48 sont ensuite comparés aux numéros de série 46 ou adresses 47 des cartes 21 et le micro-processeur 9 n'autorise la délivrance d'un message à un utilisateur que si ces numéros correspondent au complément d'adresse 48.

L'autorisation selon l'invention n'est donc donnée que si un ou plusieurs des tests suivants est réussi: présence de carte - carte authentique - authentification porteur - validité en date - nombre d'unités suffisant - complément d'adresse. Selon l'invention l'autorisation peut aussi n'être donnée que si une combinaison conjonctive de ces tests est réussie. Toutes les combinaisons de ces tests sont envisageables.

Dans la relation messageur - carte à puce, il est possible que le microprocesseur de la carte remplace celui du messageur: celui-ci en étant par exemple démuni, ou au moins incapable de fonctionner tant que le microprocesseur de la carte n'est pas en service. A l'opposé dans le cas d'un messageur sans carte, le circuit du messageur comporterait en fonction du besoin les circuits décrits pour la carte.

L'autorisation peut agir sur le fonctionnement du messageur au cours de toutes les étapes allant de l'émission à la délivrance du message.

Ainsi par exemple, l'absence d'autorisation peut inhiber la réception, ou le stockage ou le décryptage par une fonction prévue à cet effet.

Dans d'autres cas, le messageur peut être physiquement dans l'incapacité de fonctionner: par exemple lorsque le microprocesseur du messageur est contenu uniquement dans la carte, le messageur ne peut fonctionner que lorsque celle-ci est introduite dans le messageur et/ou qu'elle possède un solde suffisant.

Selon une variante avantageuse, le messageur peut recevoir le message mais l'utilisateur n'est averti de la réception que si une carte est introduite et qu'elle a suffisamment de crédit. Cela évite une utilisation minimale d'un messageur consistant à recevoir uniquement des signaux d'avertissement. L'avertissement peut prendre différentes formes par exemple sonore, lumineux, etc.

La carte peut être insérée de manière permanente et pour cela elle peut prendre un format réduit tel que le format "Plug in".

En cas d'un abonnement non renouvelé par un utilisateur, l'émetteur peut émettre une instruction d'inhibition du fonctionnement du messageur en question. Ceci peut être effectué de différentes manières ci-après.

L'espace 34 du message peut contenir dans l'indice 350, une donnée, de préférence cryptée, signifiant que l'utilisateur n'a pas l'autorisation. L'introduction d'un indice 350 de consommation supérieur à une valeur de tout solde existant suffit pour empêcher la délivrance du message, lorsque celle-ci est subordonnée à un crédit suffisant.

Selon une autre réalisation, le message peut contenir un espace réservé à une donnée d'autorisation émise systématiquement à chaque message, par l'émetteur lequel contrôle ainsi l'utilisation du service. Dans ce cas la vérification de l'autorisation peut consister à comparer systématiquement la donnée reçue, via le message, avec une donnée secrète et protégée contenue dans un bloc de sécurité du messageur tel qu'un module de sécurité applicatif (SAM).

Selon une variante, les appels à destination d'un utilisateur non à jour de son abonnement sont détournés ou bloqués par l'émetteur (opérateur). Cela implique que la vérification s'effectue avant la diffusion du message par l'émetteur.

Le procédé de contrôle/vérification peut comprendre à cet effet une étape consistant à comparer toutes les adresses des messageurs contenues dans les messages en attente d'être émis par l'opérateur, avec une liste d'adresses correspondant aux utilisateurs irréguliers (non à jour de leur abonnement), et à interdire l'émission lorsqu'il y a adéquation des adresses. A cet effet, sont prévus, des moyens de stockage de cette lis-

te et des moyens de comparaison informatiques au niveau de l'émetteur, par exemple un micro-ordinateur, et des moyens de sélection des messages par l'adresse 14 qui leur est associé. De tels moyens sont de type connu.

De préférence, pour mieux empêcher les fraudes, la carte peut avoir une durée de vie déterminée qu'elle soit rechargeable ou non. A la fin de la durée de vie, les nouvelles cartes peuvent comprendre de nouveaux algorithmes de sécurité.

Pour mettre en oeuvre la fonction durée de vie, la carte peut comprendre une date limite stockée en mémoire et un sous-programme prévu à cet effet. Selon ce programme, on compare la date limite à une date d'émission du message comprise dans chaque message. Lorsqu'il y a adéquation, le messageur refuse de fonctionner par exemple en refusant de délivrer le signal et/ou le message.

Revendications

1. Procédé de contrôle de l'utilisation d'un messageur (1) comportant les étapes suivantes:

- le messageur reçoit (2) des messages envoyés par un émetteur,
- on vérifie (16) que les messages reçus sont destinés au messageur, et quand c'est le cas on les mémorise (17) dans le messageur,
- puis on les délivre (45) au porteur du messageur,

caractérisé en ce que, avant de les délivrer,

- on vérifie (30, 31, 35) en plus que le porteur du messageur est autorisé à connaître ce qui est diffusé.

2. Procédé selon la revendication 1, caractérisé en ce que pour vérifier que le porteur est autorisé à connaître ce qui est diffusé,

- on vérifie un numéro d'authentification du porteur (PIN).

3. Procédé selon l'une des revendications 1 à 2, caractérisé en ce que pour vérifier que le porteur est autorisé à connaître ce qui est diffusé,

- on vérifie que le messageur comporte en mémoire (26) des unités prépayées disponibles, et
- on décompte une ou des unités dans cette mémoire pour autoriser la délivrance du message.

4. Procédé selon la revendication 3, caractérisé en ce que

- on décompte les unités en fonction (15, 33, 35) du message transmis.

5. Procédé selon l'une des revendications 3 à 4, caractérisé en ce que

- on décompte les unités en fonction d'un indice (350) de consommation contenu dans le message.

6. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que

- on met en relation (22,24) un support portable avec le messageur,
- on vérifie (30, 31, 35) avec le support portable que le porteur est autorisé à connaître ce qui est diffusé.

7. Procédé selon la revendication 6, caractérisé en ce que, le messageur étant apte à recevoir des messages pour au moins un utilisateur,

- on vérifie que les messages reçus sont destinés à au moins un porteur de support portable en comparant une information d'adresse (46, 47) de ce support avec un complément (48) d'adresse du message.

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que, les messages étant cryptés,

- on décrypte (43) les messages avant de les délivrer.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que

- on indexe (41) en mémoire les messages autorisés pour en permettre une redélivrance.

10. Procédé selon l'une des revendications 1 à 9, caractérisé en ce que

- on produit une alarme avant de délivrer les messages.

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce que

- on reçoit (2) les messages radio-électriquement,
- et on démodule (8) dans le messageur les messages radio-électriques reçus,

12. Messageur (1) comportant un circuit (2) de réception de message et un circuit (9, 10-13) de délivrance des messages reçus, caractérisé en ce qu'il

comporte un circuit (9,28) pour autoriser la délivrance des messages reçus.

13. Messageur selon la revendication 12, caractérisé en ce que le circuit pour autoriser comporte un circuit pour décompter des unités prépayées contenues dans une mémoire (26).

14. Messageur selon la revendication 12 ou la revendication 13, caractérisé en ce que le circuit pour autoriser comporte un circuit (27) pour authentifier le porteur du messageur.

15. Messageur selon l'une des revendications 12 à 14, caractérisé en ce qu'il comporte un module (50) de sécurité, ledit module contenant tout ou partie du circuit pour autoriser la délivrance des messages reçus.

16. Messageur selon la revendication 15, caractérisé en ce que le module de sécurité comporte tout ou partie d'un algorithme de décryptage.

17. Messageur selon l'une des revendications 15 à 16, caractérisé en ce que le module de sécurité comporte tout ou partie d'un circuit apte à réaliser le rechargement d'une mémoire en unités prépayées.

18. Messageur selon l'une des revendications 12 à 17, caractérisé en ce qu'il comprend un lecteur de carte à puce.

19. Messageur selon l'une des revendications 12 à 18, caractérisé en ce qu'il comprend des moyens aptes à identifier et/ou authentifier plusieurs utilisateurs.

20. Carte à puce pour récepteur radio de messages transcrits en texte sur écran à cristaux liquides, caractérisée en ce qu'un récepteur est équipé des éléments pour recevoir la carte, laquelle carte contrôlera le crédit qui ne fera fonctionner le récepteur que si le solde est suffisant pour reproduire le message, c'est-à-dire que la fonction de la carte est de donner accès au message à l'écran, ce qui sous-entend que le message est conditionné à l'insertion de la carte.

21. Carte à puce pour récepteur radio de messages transcrits en texte sur écran à cristaux liquides conformément à la revendication 20, caractérisée en ce qu'elle réalise la fonction de déchiffrage permettant de reproduire chaque message, c'est-à-dire qu'elle déchiffre un message par l'intermédiaire d'un code qui traduit le signal en un texte en langage connu.

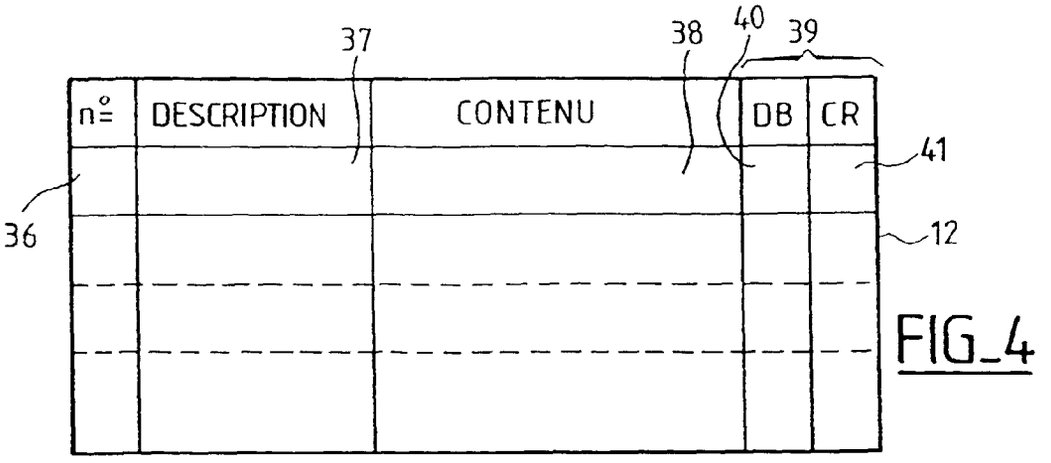


FIG_4

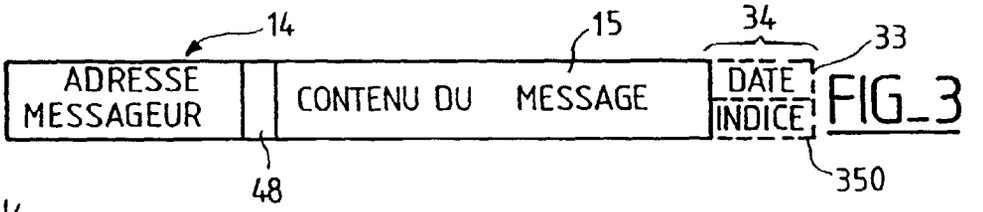
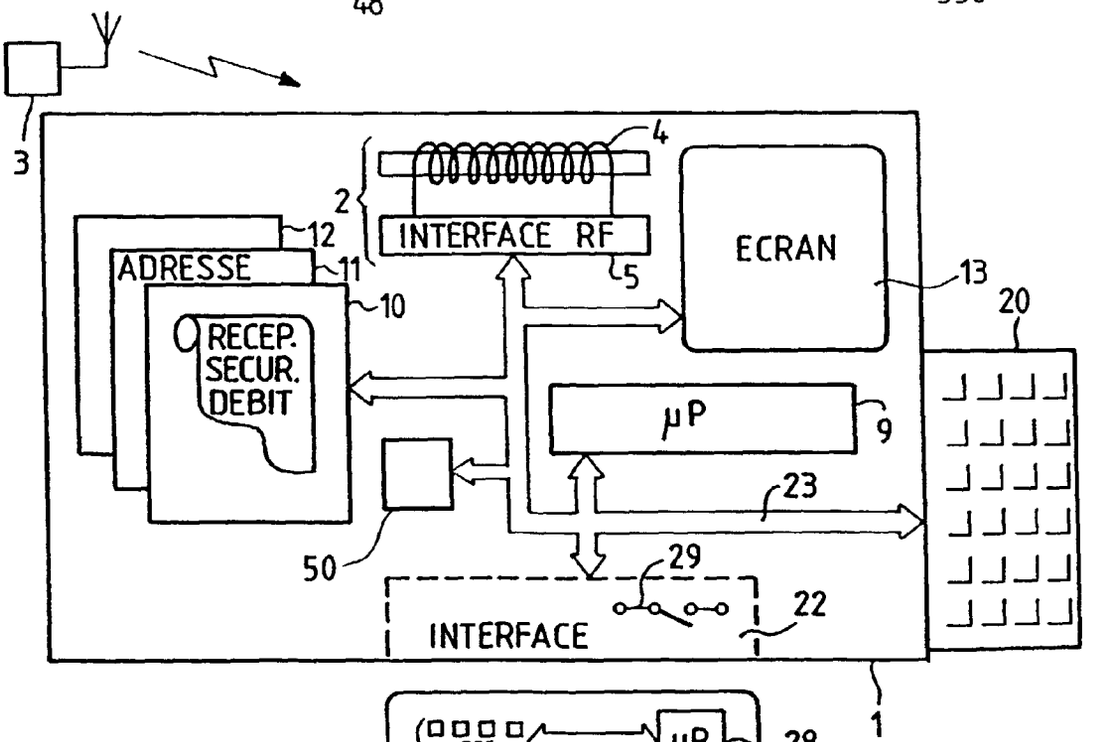


FIG_3



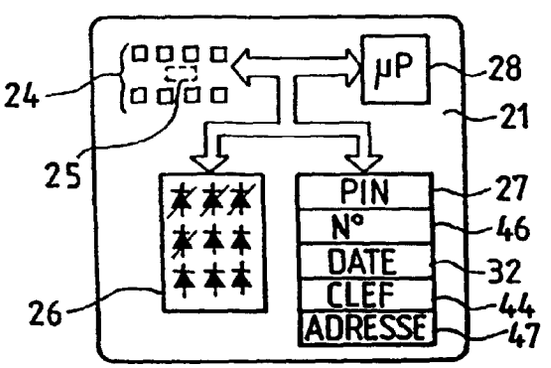


FIG_1

FIG_2

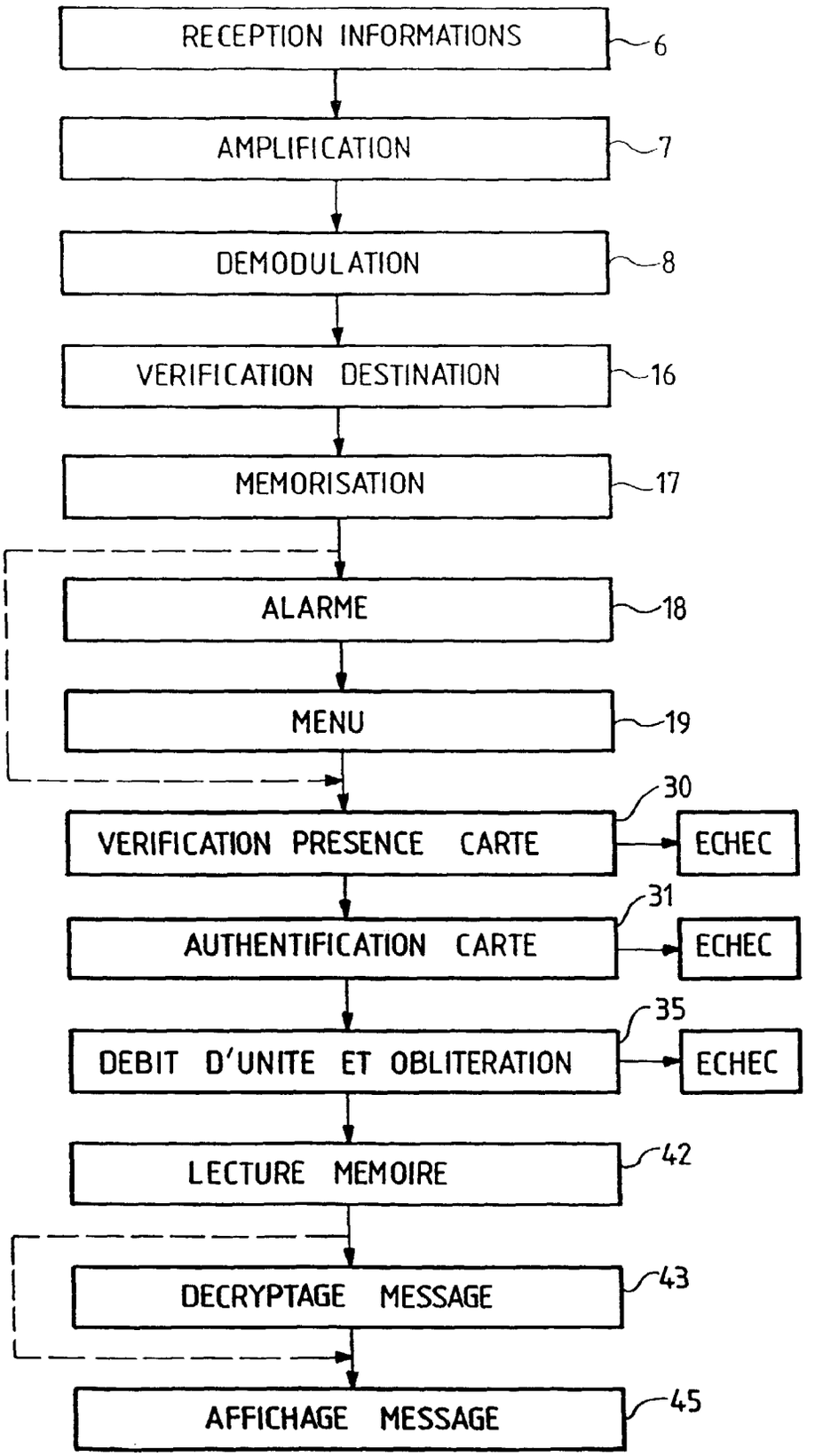
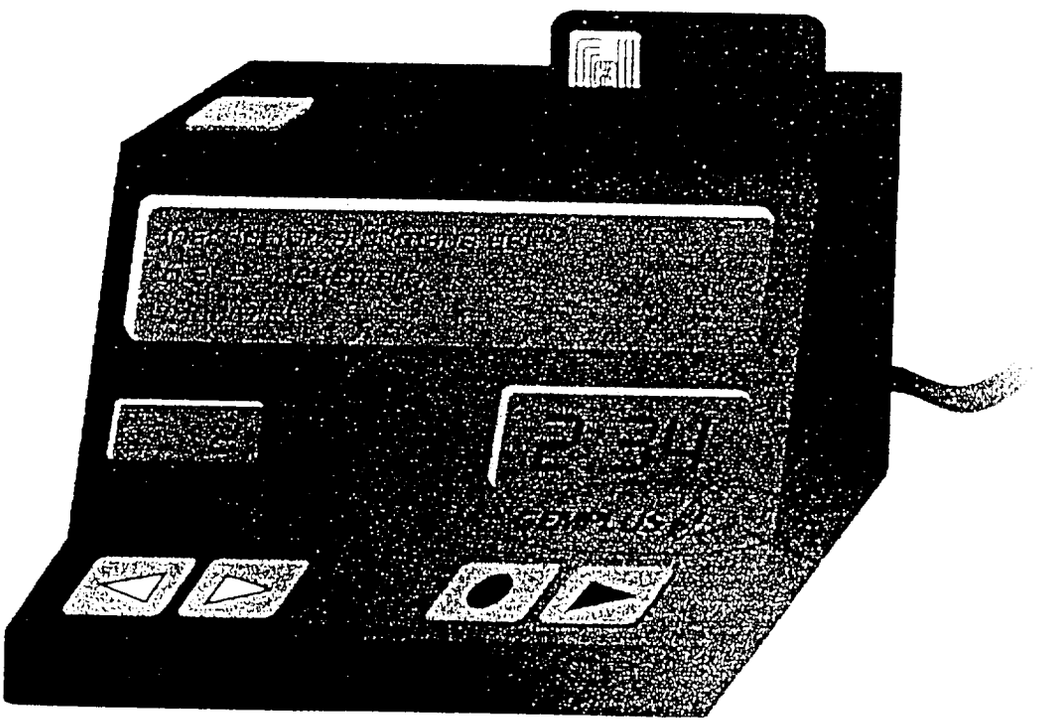

RECEPTION INFORMATIONS
6
AMPLIFICATION
7
DEMODULATION
8
VERIFICATION DESTINATION
16
MEMORISATION
17
ALARME
18
MENU
19
30
VERIFICATION PRESENCE CARTE
ECHEC
31
AUTHENTIFICATION CARTE
ECHEC
35
DEBIT D'UNITE ET OBLITERATION
ECHEC
LECTURE MEMOIRE
42
DECRYPTAGE MESSAGE
43
AFFICHAGE MESSAGE
45

FIG-5



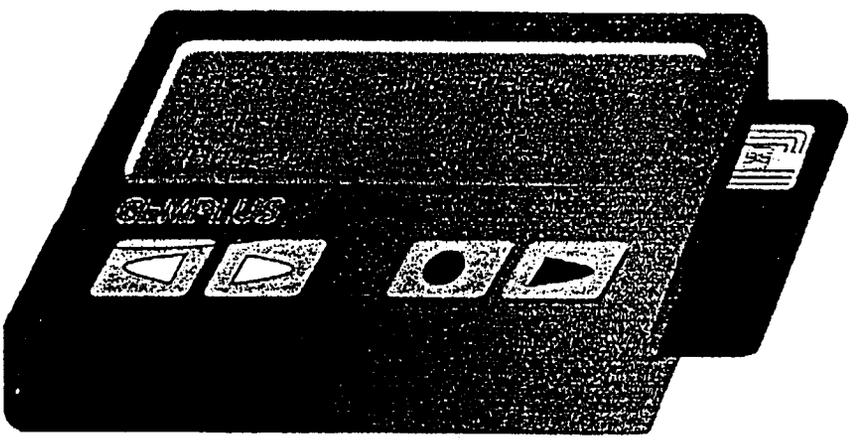


FIG-6

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 97 40 1610

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
X	GB 2 222 287 A (NEC CORP.) * abrégé; figures 1,2 * * page 3, ligne 15 - ligne 23 * * page 4, ligne 6 - ligne 22 * ---	1,6	G08B5/22
X	WO 92 17006 A (MOTOROLA,INC.) * abrégé; figure 2 * ---	1	
X	US 5 283 832 A (LOCKHART,JR. ET AL.) * abrégé; figures 5-7B * * colonne 5, ligne 13 - ligne 39 * ---	1,8,12, 14-16	
A	EP 0 538 933 A (PHILIPS ELECTRONICS UK LTD.) * abrégé; figures 1,2 * * colonne 7, ligne 30 - ligne 51 * ---	3,4,20, 21	
A	GB 2 267 168 A (STAR PAGING MFG.LTD.) * page 19, ligne 19 - ligne 24 * ---	8,16	
A	EP 0 360 228 A (CASIO COMPUTER COMPANY LTD.) * abrégé; figure 16 * * colonne 23, ligne 15 - ligne 19 * * colonne 23, ligne 32 - ligne 50 * ---	13,17	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6) G08B H04Q
A	US 5 414 418 A (ANDROS,JR.) * abrégé; figures 1-5 * * colonne 4, ligne 66 - colonne 5, ligne 9 * -----	19	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
BERLIN	8 octobre 1997	Danielidis, S

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)