(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 720 176**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 10197**

(51) Int Cl⁶ : G 06 F 17/60, H 04 M 1/66

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 19.08.94.

(30) **Priorité** : 19.05.94 CN 94105095; 30.06.94 GB 9413204.

(43) **Date de la mise à disposition du public de la demande** : 24.11.95 Bulletin 95/47.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *WONG Kam-Fu* — CN.

(72) **Inventeur(s)** : WONG Kam-Fu.

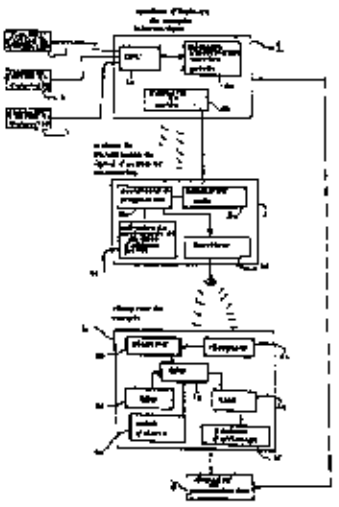
(73) **Titulaire(s)** :

(74) **Mandataire** : Cabinet Martinet & Lapoux.

(54) Système de sécurité évitant l'utilisation frauduleuse de cartes de crédit ou de téléphones cellulaires volés.

(57) Un système de sécurité pour empêcher des transactions frauduleuses comprend un dispositif d'action de transaction (1) pour enregistrer une transaction tentée et un moyen de communication (2, 3, 4) pour alerter une personne autorisée à réaliser cette transaction de la transaction tentée. Cette personne autorise ou interrompt alors la transaction tentée.

Le système de sécurité réduit ou élimine l'utilisation frauduleuse de carte de crédit ou de téléphone cellulaire volés.



FR 2 720 176 - A1

La présente invention concerne un système de sécurité et plus particulièrement un système de sécurité avec lequel un possesseur de bonne foi peut empêcher d'autres personnes d'utiliser sa carte de crédit volée et/ou son téléphone mobile volé.

Dans la société moderne, de plus en plus de transactions sont effectuées au moyen de paiements monétiques immédiats. Par exemple, lorsque des personnes font des achats, utilisent un téléphone mobile privé ou un téléphone cellulaire pour réaliser un appel local, un appel longue distance ou un appel international, elles règlent alors la facture mensuellement ou trimestriellement. On utilise également de nombreuses cartes monétiques telles que des cartes de crédit, cartes de débit, cartes de club, cartes de téléphone et similaires. Toutes ces transactions sont soit débitées instantanément sur le compte du possesseur ou sont additionnées à une facture mensuelle/trimestrielle pour le possesseur. Les différentes transactions incluent également d'aller au restaurant, à l'hôtel, de payer un logement, d'acheter des billets d'avion ou des billets de train. Après une période de temps, les factures sont réglées par débit direct, paiement par chèque ou similaire.

On utilise également des codes secrets privés, des numéros d'identification personnels pour autoriser une transaction. Un téléphone, un ordinateur ou un distributeur de billets peut être utilisé en entrant un numéro d'identification personnel pour autoriser une transaction.

Lorsque des consommateurs utilisent un moyen de paiement monétique immédiat pour payer des factures et similaires, ils n'ont pas besoin d'avoir beaucoup d'espèces avec eux. Ainsi le consommateur a moins de risque de perdre son argent et n'a pas les inconvénients de transporter de l'argent et est exposé à moins de contact avec des billets de banque sales que des gens ont touchés. Cependant, il y a des problèmes et des risques associés aux paiements monétiques immédiats. Les transactions par cartes de crédit et les appels téléphoniques cellulaires sont fondés sur l'utilisation de la technologie électronique moderne, de la technologie informatique et de la technologie de communication par modem. Ces technologies sont difficiles à protéger avec des procédés de sécurité connus. Des criminels utilisent une technologie avancée pour voler des cartes de crédit de consommateurs, des téléphones cellulaires et pour obtenir des informations sur les codes secrets de consommateurs et les numéros d'identification personnels afin de réaliser des transactions par carte de crédit falsifiée et des appels par téléphone cellulaire. L'augmentation de l'utilisation de moyens de paiement monétique immédiat augmente ces problèmes.

Des exemples de paiements monétiques immédiats illégaux sont présentés ci-après.

Lorsqu'un téléphone mobile d'un consommateur est perdu ou volé, celui qui le trouve ou le voleur peut copier les caractéristiques internes du téléphone mobile afin de réaliser une reproduction illégale du téléphone, telle que tout appel futur effectué avec le téléphone mobile soit facturé au possesseur de bonne foi du téléphone.

Lorsque des cartes de consommateur telles que des cartes de crédit sont volées par un voleur ou les informations contenues sur la carte de crédit sont volées par un voleur et une carte illégale reproduite d'après celles-ci, des commerçants ou des banques peuvent accepter la carte de crédit volée ou la carte de crédit reproduite provoquant des pertes pour le consommateur ou les banques. On enregistre actuellement vingt millions de cartes de crédit perdues ou volées par an. La quantité d'argent perdu en raison de la fraude sur les cartes de crédit tourne autour de plusieurs centaines de millions de dollars. Jusqu'à maintenant, il n'y avait pas de moyen réellement efficace pour résoudre les problèmes mentionnés.

Un objectif de la présente invention est de résoudre ou d'améliorer les problèmes ci-dessus mentionnés.

En conséquence, la présente invention fournit un système de sécurité pour empêcher des transactions frauduleuses, caractérisé en ce qu'il comprend un dispositif d'action de transaction pour enregistrer une transaction tentée, et un moyen de communication pour alerter une personne autorisée à réaliser cette transaction de la transaction tentée.

La présente invention fournie une protection des transactions par paiement monétique immédiat. Même si le véritable possesseur d'une carte de crédit ou d'un téléphone mobile n'est pas averti que sa carte ou son téléphone mobile a été volé(e) ou est perdu(e), il peut savoir immédiatement si quelqu'un utilise la carte volée ou le téléphone mobile pour réaliser une transaction frauduleuse. Le véritable possesseur peut

alors prendre une décision en fonction du fait que la transaction est légale ou illégale. Si la transaction est illégale, alors une action immédiate peut être entreprise pour informer la banque, le commerçant, la compagnie de téléphone afin d'interrompre la transaction illégale, de refuser le paiement des biens, d'interrompre l'utilisation de la carte de crédit ou d'interrompre l'utilisation du téléphone mobile de sorte que toutes pertes du véritable possesseur, de la banque ou du commerçant sont réduites et même éliminées. Il est envisageable que le procédé conforme à la présente invention réduise ou élimine ainsi ce type de délit commercial.

Un moyen de communication supplémentaire est prévu pour permettre à la personne autorisée d'autoriser ou d'empêcher la transaction tentée.

De préférence est également prévu un système d'écriture de compte informatique qui est en communication avec le dispositif d'action de transaction pour recevoir des détails de la transaction tentée et qui est utilisable pour communiquer les détails de la transaction tentée à la personne autorisée.

De manière à informer immédiatement le véritable possesseur qu'une action de transaction de paiement monétique immédiat le concernant survient, le système de sécurité peut comprendre un dispositif d'action de transaction, un système d'écriture de compte informatique, une station de transmission de signal d'action de transaction, et un récepteur de compte.

Le dispositif d'action de transaction peut comprendre un dispositif de lecture de carte de crédit pour lire une carte de crédit, une carte de

membre, une carte de club, une carte magnétique, ou analogue, pour régler le paiement ou compranant différents types de téléphones mobiles tels que téléphone cellulaire, téléphone de voiture, téléphone à code secret, ou analogue. Lorsqu'une action de transaction survient, le dispositif d'action de transaction crée une information d'action de transaction et transfère l'information d'action de transaction à un système d'écriture de compte informatique correspondant.

Le système d'écriture de compte informatique traite des signaux d'information d'action de transaction communiqués par le dispositif d'action de transaction, compare le code d'adresse privé du véritable possesseur avec le code dans la mémoire d'information secrète privée, et transmet ces signaux d'information à la station de transmission de signal d'action de transaction.

La station de transmission de signal d'action de transaction peut comprendre un éditeur de code, un contrôleur de programme, une mémoire de sauvegarde et de code d'adresse privé et un émetteur.

L'éditeur de code combine le code d'adresse privé du véritable possesseur dans la mémoire de sauvegarde et de code d'adresse privé, et code les différents signaux d'information d'action de transaction reçus. Le contrôleur de programme ordonne à l'émetteur d'émettre immédiatement les signaux codés des signaux d'information d'action de transaction combinés avec le code d'adresse privé.

Le récepteur de compte peut comprendre un récepteur, un décodeur, une mémoire morte d'identification, une mémoire vive, une unité d'alerte, un panneau d'affichage et une unité centrale de traitement. Le récepteur reçoit les

signaux d'information codés relatifs au code d'adresse privé transmis depuis la station de transmission de signal d'action de transaction et les transmet au décodeur qui les décode sous le contrôle de l'unité centrale, pour déclencher l'unité d'alerte pour fournir un son, une vibration, un éclair de diode, ou similaire afin d'indiquer une information arrivant et afficher l'information d'action de transaction sur le panneau d'affichage avec des symboles, nombres, mots ou caractères, et pour stocker des informations d'action de transaction dans la mémoire vive pour utilisation ultérieure.

Le système d'écriture de compte informatique peut être un système d'écriture de compte informatique de carte de crédit utilisé dans une banque avec un dispositif de sortie additionnel ou peut être un système informatique de compte de téléphone utilisé dans une compagnie de téléphone avec un dispositif de sortie additionnel.

La station de transmission de signal d'action de transaction peut être une station de recherche de personnes ou un système de recherche de personnes.

Le récepteur de compte peut être un récepteur d'appel portable, un récepteur de table, une montre, un téléphone mobile, un ordinateur de téléphone général ou un dispositif électrique ou électronique spécialement conçu pour recevoir des signaux d'information d'action de transaction et afficher l'information d'action de transaction et a une unité d'alerte pour alerter le véritable possesseur concerné.

La mémoire d'identification du récepteur de compte a de préférence au moins un code d'identification ou un code d'adresse privé écrit par la station de transmission de signal d'action de

transaction et/ou des codes d'adresse supplémentaires tels qu'un code d'adresse T écrit par une compagnie de téléphone et/ou un code d'adresse B écrit par un système d'écriture de compte informatique de banque.

La station de transmission de signal d'action de transaction peut envoyer différents symboles d'affichage pour différentes actions de transactions tels que "BK" pour une action de transaction de cartes de crédit, "ST" pour une action de transaction de téléphone cellulaire, "KT" pour une action de transaction de téléphone à code secret, des nombres concernant la valeur monétaire de l'action de transaction, et des symboles et nombres et mots et caractères concernant le lieu de l'action de transaction, le numéro de téléphone appelé et similaire.

Une pluralité de systèmes d'écriture de compte informatique et de stations de transmission de signal d'action de transaction, de préférence connectés dans un réseau, peuvent être prévus afin que la zone de couverture de signal transmise par la station de transmission de signal d'action de transaction soit agrandie si nécessaire.

Un centre de traitement informatique de signal d'action de transaction peut être prévu pour augmenter le nombre de signaux d'action de transaction et augmenter la vitesse de traitement.

L'invention concerne également un procédé d'utilisation du système de sécurité selon l'invention pour informer immédiatement le véritable possesseur qu'une action de transaction de paiement monétique le concernant se produit. Le procédé comprend les étapes suivantes : pendant la durée d'une action de transaction transmettre une

information concernant l'action de transaction au véritable possesseur, permettre au véritable possesseur de prendre une décision si l'action de transaction est autorisée ou non et informer le dispositif d'action de transaction de la décision du véritable possesseur.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un organigramme d'utilisation d'un système de sécurité selon la présente invention ;
- la figure 2 est un bloc-diagramme schématique d'un système de sécurité selon la présente invention;
- les figures 3-1 et 3-2 sont des représentations schématiques de codes d'adresse stockés dans des récepteurs de compte ;
- la figure 4 est un bloc-diagramme schématique d'un autre système de sécurité selon la présente invention ;
- la figure 5 est un bloc-diagramme schématique d'encore un autre système de sécurité conforme à la présente invention ;
- la figure 6 est un bloc-diagramme schématique d'un centre de traitement informatique de signaux d'action de transaction pour utilisation avec un système de sécurité selon la présente invention ; et
- la figure 7 est un bloc-diagramme schématique d'une unité d'information de la police pour utilisation avec un système de sécurité selon la présente invention.

La figure 1 représente un organigramme montrant les étapes d'utilisation d'un système de sécurité conforme à la présente invention. Lorsqu'une personne utilise un téléphone mobile ou un téléphone de voiture pour effectuer un appel ou lorsque quelqu'un tente de réaliser une transaction en utilisant une carte de crédit, alors une transaction de paiement monétique immédiat se produit. Une telle transaction est appelée dans la suite une "action de transaction". La numérotation sur le téléphone mobile alerte un système d'écriture de compte informatique de la compagnie de téléphone exploitant le téléphone mobile, du fait que le téléphone mobile est en train d'être utilisé et commence à calculer et à enregistrer le temps, le lieu, la distance et le coût de l'appel téléphonique. Lorsque quelqu'un utilise une carte de crédit pour effectuer une transaction et que la carte de crédit est lue par un dispositif de lecture de carte de crédit sur le point de vente, alors un système d'écriture de compte informatique correspondant dans une banque ou un magasin de détail commence à fonctionner pour enregistrer la transaction sur la carte. A cet instant, le système d'écriture de compte informatique, par exemple dans une banque, crée un signal d'action de transaction. Le système d'écriture de compte informatique évalue à partir des informations fournies le code d'adresse privé du véritable possesseur de la carte de crédit ou du téléphone. Un dispositif de sortie dans le système d'écriture de compte informatique applique un signal incluant le signal d'action de transaction à une station de transmission de signal d'action de transaction au moyen d'une transmission radioélectrique, du réseau téléphonique ou d'un autre câble de communication.

La station de transmission d'action de transaction traite les signaux reçus et transmet alors de tels signaux sur une grande zone. Le véritable possesseur de la carte de crédit ou du téléphone mobile porte un récepteur de compte qui reçoit le signal transmis incluant le signal d'action de transaction afin d'alerter le véritable possesseur qu'une action de transaction indiquant une transaction est en train d'être réalisée par quelqu'un qui utilise la carte de crédit ou le téléphone du possesseur.

Par exemple, le récepteur de compte peut posséder un dispositif d'affichage qui peut indiquer le signe "B25" pour indiquer que la carte de crédit du possesseur est en train d'être utilisée dans une transaction d'un montant de vingt cinq dollars. D'autres exemples peuvent être l'indication "STBJ" indiquant que le téléphone cellulaire du possesseur est utilisé pour appeler Beijing.

Lorsque le possesseur reçoit le signal via le récepteur de compte, le possesseur peut prendre une décision immédiate si l'action de transaction est réalisée légalement par lui-même ou est en train d'être accomplie illégalement par un tiers, par exemple si le téléphone en train d'être utilisé pour réaliser l'appel est un téléphone reproduit illégalement ou si la carte de crédit est une reproduction falsifiée utilisant un code volé. En fonction des instructions en cours, à moins que le système d'écriture de compte informatique reçoive un ordre contraire, par exemple dans les deux ou trois minutes, le système d'écriture de compte informatique autorise l'action de transaction. Si le véritable possesseur pense que l'action de transaction est illégale, il peut immédiatement utiliser toute forme

de dispositif de communication, tel qu'un téléphone, pour informer le système d'écriture de compte informatique concerné que l'action de transaction est illégale. Si c'est le cas, alors le système d'écriture de compte informatique renvoie un signal prédéterminé vers le point de vente ou la banque où l'action de transaction a lieu pour ordonner au dispositif d'action de transaction de refuser l'action de transaction ou d'interrompre l'action de transaction. Par exemple, le signal sur l'écran du dispositif de lecture de carte de crédit au point de vente peut indiquer que la carte est refusée ou le signal autorisant le téléphone cellulaire à fonctionner est interrompu pour terminer l'appel. De cette manière, le véritable possesseur, la banque, la compagnie de téléphone et les commerçants évitent ou réduisent toute perte due à de telles actions de transaction illégales. Les délits commerciaux de cette nature peuvent ainsi être éliminés. Toute la procédure prend une à deux minutes environ ou parfois encore moins.

Dans la figure 2 est représenté un système de sécurité comprenant une pluralité de dispositifs d'action de transaction 1, une pluralité de systèmes d'écriture de compte informatique correspondants 2, une ou plusieurs stations de transmission de signaux d'action de transaction 3, une pluralité de récepteurs de compte 4 et un ou plusieurs dispositifs de communication 5.

Les dispositifs d'action de transaction 1 tels que mentionnés précédemment peuvent être des dispositifs variés tels que des lecteurs des cartes de crédit, des téléphones cellulaires, des distributeurs de billets ou similaire, tous étant des

dispositifs de paiement monétique immédiat. Les dispositifs d'action de transaction 1 génèrent des signaux d'action de transaction lorsqu'une transaction est effectuée et envoient les signaux d'action de transaction au système d'écriture de compte informatique 2.

Le système d'écriture de compte informatique 2 inclut une unité centrale de traitement (CPU) 2a, un dispositif de sortie 2b et une mémoire d'information secrète privée 2c. L'unité centrale 2a est utilisée pour enregistrer l'information d'action de transaction reçue dans le signal d'action de transaction depuis le dispositif d'action de transaction 1. Par exemple, si le système d'écriture de compte informatique est dans un ordinateur de banque, l'information va être le lieu d'utilisation de la carte de crédit, la durée et la date de la transaction, la valeur de la transaction, le numéro de la carte, ou si l'unité centrale est dans l'ordinateur d'une compagnie de téléphone, l'information va être le numéro du téléphone cellulaire, au moyen duquel est effectué un appel et le numéro de téléphone appelé, la durée et la date, le temps passé sur l'appel, etc. L'unité centrale 2a va se référer au code d'adresse privé stocké dans la mémoire d'information secrète privée 2c, traiter les signaux reçus depuis le dispositif d'action de transaction 1 et envoyer les signaux traités incluant les signaux d'action de transaction au dispositif de sortie 2b. Le dispositif de sortie 2b applique immédiatement tous les signaux d'information à la station de transmission de signal d'action de transaction 3 au moyen d'une transmission sans fil, du réseau téléphonique ou de câbles de communication appropriés.

La station de transmission de signal d'action de transaction 3 inclut un éditeur de code 3a, un contrôleur de programme 3b, une mémoire de sauvegarde et de code d'adresse privé 3c et un émetteur 3d qui prend les signaux d'information entrants et vérifie si le code secret privé du véritable possesseur est le même que le code d'adresse privé dans la mémoire 3c pour coder celui-ci dans l'éditeur de code 3a. Le contrôleur de programme 3b transfère les signaux codés à l'émetteur 3d qui émet immédiatement l'information d'action de transaction codée vers une zone de couverture dans laquelle le véritable possesseur est situé de sorte que les signaux d'information d'action de transaction peuvent être reçus par le véritable possesseur.

Le véritable possesseur doit avoir un récepteur de compte 4 pour recevoir l'information d'action de transaction. Le récepteur de compte 4 comprend un récepteur 4a, un décodeur 4b, une mémoire vive (RAM) 4c, une mémoire morte d'identification (ROM) 4d, une unité d'alerte 4e, un panneau d'affichage 4f et une unité centrale de traitement (CPU) 4g.

Le récepteur 4a reçoit les signaux d'information d'action de transaction codés transmis par la station de transmission de signal d'action de transaction 3 et envoie ceux-ci au décodeur 4b. Le décodeur 4b se réfère au code d'adresse privé du véritable possesseur dans la mémoire morte d'identification 4d, et décode les signaux d'information d'action de transaction et envoie les signaux à l'unité centrale 4g. L'unité centrale 4g commande le programme et déclenche l'unité d'alerte 4e, le panneau d'affichage 4f et la mémoire vive 4c. L'unité d'alerte 4e peut comprendre une unité sonore, une unité de vibration, une unité d'affichage à cristaux liquides ou

similaire et est utilisée pour alerter le véritable possesseur du fait qu'une action de transaction le concernant se produit. Le panneau d'affichage 4f montre l'information concernant l'action de transaction. La mémoire vive 4c est une mémoire pour stocker temporairement l'information d'action de transaction. Lorsque le véritable possesseur a besoin de l'information d'action de transaction, il peut utiliser l'information stockée dans la mémoire vive 4c. Lorsque le véritable possesseur n'a plus besoin de cette information, il peut entrer des instructions pour éliminer l'information stockée dans la mémoire 4c.

Le véritable possesseur peut juger d'après l'affichage 4f si l'action de transaction est légale ou illégale. Si l'action de transaction est réalisée par le véritable possesseur lui-même, tel qu'un dirigeant de société utilisant une carte de crédit de société pour payer une note concernant une invitation de clients de la société à dîner, l'action de transaction est légale. Le véritable possesseur de la carte de crédit n'a pas besoin de réaliser d'action supplémentaire. L'action de transaction sera autorisée comme précédemment décrit et peut se poursuivre.

Si les symboles représentés sur l'affichage 4f laissent le véritable possesseur penser que l'action de transaction est illégale, telle qu'une action de transaction impliquant quelqu'un utilisant le téléphone cellulaire du possesseur et le téléphone cellulaire ayant juste été perdu, ou si quelqu'un utilise une carte de crédit falsifiée avec des informations volées relatives au possesseur pour payer une note, alors le véritable possesseur peut utiliser tout dispositif de communication tel qu'un

téléphone pour informer le système d'écriture de compte informatique correspondant 2 pour refuser ou interrompre l'action de transaction illégale. Le système d'écriture de compte informatique 2 va refuser ou interrompre l'action de transaction au dispositif d'action de transaction 1, selon l'ordre selon lequel le véritable possesseur envoie les signaux d'instructions. Par exemple, lorsque le dispositif d'action de transaction 1 est un lecteur de carte 1, en indiquant audit dispositif de refuser le paiement ou en faisant revenir le téléphone mobile utilisé à son état initial et interrompant l'appel. De cette manière, les pertes du véritable possesseur de la carte de crédit et/ou du téléphone mobile peuvent être réduites comme peuvent l'être les pertes de la banque concernée et de la compagnie de téléphone. De cette manière, les délits commerciaux impliquant l'utilisation illégale de transactions par paiement monétique immédiat peuvent être réduits ou éliminés. Un tel système contribue à de grands bénéfices à la société et à l'économie.

Le système d'écriture de compte informatique 2 peut être le système d'écriture de compte informatique actuel utilisé dans les banques ou les compagnies de téléphone avec un dispositif de sortie additionnel 2b. Le dispositif de sortie 2b est utilisé pour transférer l'information d'action de transaction du véritable possesseur à la station de transmission de signal d'action de transaction 3. La station de transmission de signal d'action de transaction 3 peut être un système de recherche de personnes largement utilisé ou une autre forme de station de transmission. Le récepteur de compte peut être un récepteur d'appel, un récepteur d'appel portable, un récepteur d'appel de table ou une montre

ou horloge avec une unité centrale 4g, une unité d'alerte immédiate 4e et un panneau d'affichage 4f pour recevoir et afficher des signaux d'information d'action de transaction. En variante, le récepteur de compte peut être un téléphone mobile, un téléphone normal ou un ordinateur ou un dispositif électrique ou électronique spécialement conçu pour recevoir et afficher des signaux d'information d'action de transaction et pour attirer l'attention du véritable possesseur vers ceux-ci au moyen de l'unité d'alerte 4e.

La figure 3 représente deux exemples de récepteurs de compte 4 et la mémoire morte d'identification respective ROM 4d du récepteur de compte 4.

Le récepteur de compte 4 inclut un code d'adresse d'identité privé écrit dans la mémoire morte d'identification 4d par la station de transmission de signal d'action de transaction 3. Le code d'adresse est similaire à celui donné à chaque récepteur d'appel utilisé de sorte que chaque récepteur d'appel peut être identifiable sélectivement par la station de recherche de personnes. Grâce au code d'adresse, un message depuis la station de transmission de signal d'action de transaction 3 ne sera pas reçu par tous les récepteurs de compte 4 mais seulement par le récepteur de compte 4 associé au code d'adresse de cette personne. Le code d'adresse peut être un nombre ayant plusieurs chiffres tels qu'un nombre à huit chiffres, un nombre à dix chiffres, etc. La personne portant le récepteur de compte 4 n'a pas besoin de connaître le code d'adresse d'identité privé. Le code d'adresse d'identité privé peut être écrit à l'avance

dans la mémoire morte d'identification 4d par le fabricant du récepteur de compte ou peut être écrit par la station de transmission de signal d'action de transaction 3 ou par le possesseur qui change le code d'adresse manuellement et informe ensuite la station de transmission de signal d'action de transaction. D'une manière générale, il y a au moins un code d'adresse privé dans la mémoire morte d'identification 4d du récepteur de compte 4 comme représenté à la figure 3-1. Le récepteur de compte 4 doit être capable de recevoir des signaux d'action de transaction, par exemple des signaux d'action de transaction des différentes cartes de crédit, lorsque le dispositif de sortie 2b du système d'écriture de compte informatique de la banque transmet des signaux d'action de transaction, un code distinct identifiant le possesseur correct de la carte de crédit doit être ajouté. Par exemple, le code distinct d'une personne est CB12450 et le signal d'action de transaction est B25. Le panneau d'affichage 4f du récepteur de compte 4 affiche les symboles CB12450 + B25.

Le récepteur de compte représenté à la figure 3-2 peut recevoir des signaux d'action de transaction depuis l'utilisation d'une carte de crédit. La banque concernée qui traite les cartes de crédit peut écrire dans son système informatique de banque un code d'adresse B dans la mémoire morte d'identification 4b du récepteur de compte qui peut distinguer d'autres cartes de crédit. Pour toutes les cartes de crédit, la banque écrit un code d'adresse B pour le véritable possesseur, c'est-à-dire le possesseur de la carte de crédit dans la mémoire morte d'identification du récepteur de compte 4. De la même manière, pour tout téléphone mobile tel qu'un téléphone cellulaire, la compagnie de téléphone utilise le système d'écriture

de compte informatique 2 pour écrire un code d'adresse T dans la mémoire morte d'identification 4d du récepteur de compte 4 pour le véritable possesseur. Puis, dans le récepteur de compte 4, il y a au moins un code d'identification écrit par la station de transmission de signal d'action de transaction, un code d'adresse B écrit par la banque respective et un code d'adresse T écrit par la compagnie de téléphone respective.

Bien sûr, tous ces codes peuvent être écrits par un menu de récepteur d'appel si le récepteur de compte comprend un récepteur d'appel. Ainsi, il y a habituellement deux ou trois codes d'adresse dans le récepteur de compte 4. Ainsi, lorsque l'action de transaction se produit telle que les exemples mentionnés ci-dessus, le panneau d'affichage 4f du récepteur de compte 4 affiche seulement B25 au lieu de CB12450 + B25. Puisque le code d'adresse a déjà été écrit dans le récepteur de compte 4, le symbole CB12450 peut être évité et plus de symboles d'information d'action de transaction peuvent être présentés par le panneau d'affichage 4f. Plus d'informations d'action de transaction peuvent ainsi être présentées au véritable possesseur.

La figure 4 illustre une réalisation similaire à celle représentée à la figure 2 dans laquelle une pluralité de dispositifs d'action de transaction sont chacun associés à un système d'écriture de compte informatique correspondant, laquelle pluralité de systèmes d'écriture de compte informatique passe par une unique station de transmission de signal d'action de transaction 3. Puisque la station de transmission de signal d'action de transaction 3 est reliée à une pluralité de systèmes d'écriture de compte

informatique 2, l'éditeur de code 3a peut augmenter la capacité de fonctionnement et la vitesse de traitement de l'information d'action de transaction.

Tout le processus depuis l'apparition de l'action de transaction jusqu'à l'affichage de l'information d'action de transaction sur le récepteur de compte 4 peut prendre seulement quelques secondes.

La figure 5 représente une autre réalisation de la présente invention dans laquelle plusieurs systèmes d'écriture de compte informatique passent par un nombre correspondant de stations de transmission de signal d'action de transaction 3 pour transmettre l'information d'action de transaction.

Les signaux d'information d'action de transaction peuvent être transmis parmi les stations de transmission de signal d'action de transaction de sorte que les signaux d'information d'action de transaction sont transmis sur plusieurs zones, plusieurs régions dans un pays, ou plusieurs pays et même dans tout le monde.

La figure 6 représente une autre réalisation de la présente invention dans laquelle une pluralité de systèmes d'écriture de compte informatique et une pluralité de stations de transmission de signal d'action de transaction 3 sont reliés par un unique centre de traitement informatique de signal d'action de transaction 6 qui traite un grand nombre de signaux d'information d'action de transaction venant de tous les systèmes d'écriture de compte informatique 2 et qui transfère immédiatement les signaux aux stations de transmission de signal

d'action de transaction correctes pour transmettre de telles informations.

La figure 7 représente encore une autre réalisation de la présente invention qui inclut une unité d'information de la police 2f dans le système d'écriture de compte informatique. Lorsqu'un véritable possesseur a indiqué qu'une action de transaction est illégale et l'action de transaction est à refuser ou à interrompre, alors avant qu'une telle instruction soit envoyée au dispositif d'action de transaction, l'unité d'information de la police est activée et informe la police qu'une action de transaction illégale a lieu et où ladite action de transaction a lieu de sorte que la police peut entreprendre immédiatement une action pour appréhender la personne agissant illégalement.

Bien sûr, un récepteur de compte plus sophistiqué 4 peut être utilisé qui peut afficher plus d'informations telles que le type de transaction qui est mené, quelle carte est utilisée, le numéro de la carte de crédit, la quantité d'argent qui va être dépensée dans la transaction et le lieu d'utilisation de la carte de crédit, ou quel type de téléphone est utilisé, qu'il soit téléphone mobile, de voiture, cellulaire ou à code secret, le lieu et la date de l'appel téléphonique et le numéro appelé. Toutes ces informations peuvent être affichées au moyen de symboles, mots et caractères sur un dispositif d'affichage sur le récepteur de compte 4. Ainsi, le véritable possesseur peut entreprendre des actions nécessaires pour interrompre l'action de transaction illégale.

En conséquence, lorsque des transactions de paiement monétique immédiat tels que des paiements

par carte de crédit ou utilisation d'un téléphone mobile, etc, surviennent, le procédé et le système de sécurité selon la présente invention fournissent au véritable possesseur de la carte de crédit ou du téléphone mobile une connaissance immédiate qu'une transaction survient de sorte que le véritable possesseur peut entreprendre l'action appropriée.

Il doit être noté que lorsqu'une transaction de paiement monétique immédiat survient, le système d'écriture de compte informatique correspondant va fonctionner. Le système d'écriture de compte informatique peut être le système informatique de la banque ou un système informatique d'une société de service tel que le système informatique d'une compagnie de téléphone cellulaire. Tous les systèmes informatiques ci-dessus sont désignés ici par "système d'écriture de compte informatique". Le système d'écriture de compte informatique délivre des signaux d'information qui incluent qu'une action de transaction (transaction de paiement monétique immédiat) se produit et le code d'adresse privé du véritable possesseur enregistré dans le système à la station de transmission de signal d'action de transaction, par un procédé de communication tel que communication sans fil, transmission de l'information par un réseau de lignes téléphoniques ou un câble de communication approprié.

La station de transmission de signal d'action de transaction envoie immédiatement les signaux d'information d'action de transaction selon le code d'identification du véritable possesseur à la station dans la zone de couverture appropriée. Le véritable possesseur peut recevoir rapidement les signaux par un récepteur de compte qu'il porte sur lui lorsqu'une action de transaction le concernant se produit. Selon

les signaux reçus, le véritable possesseur peut juger s'il doit entreprendre une action ou non. Si pendant une durée prédéterminée telle que deux ou trois minutes, le véritable possesseur n'entreprend aucune action, il est supposé que le véritable possesseur accepte l'action de transaction et l'action de transaction est par conséquent autorisée. Si le véritable possesseur pense que l'action de transaction est une utilisation illégale d'une carte de crédit volée ou similaire, il peut utiliser n'importe quel moyen de communication nécessaire pour informer le système d'écriture de compte informatique de l'utilisation illégale.

Le système d'écriture de compte informatique peut renvoyer des signaux à l'endroit où l'action de transaction a lieu tel qu'au lecteur de carte de crédit pour refuser le paiement, ou des signaux peuvent être renvoyés au téléphone mobile pour interrompre la liaison téléphonique. Ainsi, les pertes du véritable possesseur et de la société de service concernée ou de la banque peuvent être réduites ou éliminées. Les délits commerciaux d'utilisation frauduleuse de cartes de crédit et/ou de téléphones cellulaires volés seront ainsi empêchés.

REVENDICATIONS

1 - Système de sécurité pour empêcher des transactions frauduleuses, caractérisé en ce qu'il comprend :

un dispositif d'action de transaction (1) pour enregistrer une transaction tentée; et

un moyen de communication (2, 3, 4) pour alerter une personne autorisée à réaliser cette transaction de la transaction tentée.

2 - Système de sécurité conforme à la revendication 1, dans lequel un moyen de communication supplémentaire est prévu pour permettre à la personne autorisée d'autoriser ou d'empêcher la transaction tentée.

3 - Système de sécurité conforme à la revendication 1 ou 2, dans lequel un système d'écriture de compte informatique (2) est prévu, lequel système d'écriture de compte informatique est en communication avec le dispositif d'action de transaction (1) pour recevoir des détails de la transaction tentée et est utilisable pour communiquer les détails de la transaction tentée à la personne autorisée.

4 - Système de sécurité conforme à l'une quelconque des revendications 1 à 3 pour informer immédiatement le véritable possesseur qu'une action de transaction de paiement monétique immédiat le concernant survient, comprenant :

un dispositif d'action de transaction (1), un système d'écriture de compte informatique (2), une

station de transmission de signal d'action de transaction (3), et un récepteur de compte (4);

le dispositif d'action de transaction (1) comprenant un dispositif de lecture de carte de crédit pour lire une carte de crédit, une carte de membre, une carte de club, une carte magnétique, ou analogue pour régler le paiement ou comprenant différents types de téléphones mobiles tels que téléphone cellulaire, téléphone de voiture, téléphone à code secret, ou analogue; lorsqu'une action de transaction survient, le dispositif d'action de transaction (1) créant une information d'action de transaction et transférant l'information d'action de transaction à un système d'écriture de compte informatique correspondant (2);

le système d'écriture de compte informatique (2) traitant des signaux d'information d'action de transaction communiqués par le dispositif d'action de transaction, comparant le code d'adresse privé du véritable possesseur avec le code dans une mémoire d'information secrète privée (2c), et transmettant ces signaux d'information à la station de transmission de signal d'action de transaction (3);

la station de transmission de signal d'action de transaction (3) comprenant un éditeur de code (3a), un contrôleur de programme (3b), une mémoire de sauvegarde et de code d'adresse privé (3c) et un émetteur (3d);

l'éditeur de code (3a) combinant le code d'adresse privé du véritable possesseur dans la mémoire de sauvegarde et de code d'adresse privé (3c) et codant les différents signaux d'information d'action de transaction reçus, le contrôleur de programme (3b) ordonnant à l'émetteur (3d) d'émettre immédiatement les signaux codés des signaux

d'information d'action de transaction combinés avec le code d'adresse privé ;

le récepteur de compte (4) comprenant un récepteur (4a), un décodeur (4b), une mémoire vive (4c), une mémoire morte d'identification (4d), une unité d'alerte (4e), un panneau d'affichage (4f) et une unité centrale de traitement (4g); le récepteur (4a) recevant les signaux d'information codés relatifs au code d'adresse privé transmis depuis la station de transmission de signal d'action de transaction (3) et les transmettant au décodeur (4b) qui les décode sous le contrôle de l'unité centrale (4g), pour déclencher l'unité d'alerte (4e) pour fournir un son, une vibration, un éclair de diode, ou similaire afin d'indiquer une information arrivant et afficher l'information d'action de transaction sur le panneau d'affichage (4f) avec des symboles, nombres, mots ou caractères, et pour stocker des informations d'action de transaction dans la mémoire vive (4c) pour utilisation ultérieure.

5 - Système de sécurité conforme à la revendication 4, dans lequel le système d'écriture de compte informatique (2) est un système d'écriture de compte informatique de carte de crédit utilisé dans une banque avec un dispositif de sortie additionnel (2b) ou est un système informatique de compte de téléphone utilisé dans une compagnie de téléphone avec un dispositif de sortie additionnel (2b).

6 - Système de sécurité conforme à la revendication 4 ou 5, dans lequel la station de transmission de signal d'action de transaction (3) est une station de recherche de personnes ou un système de recherche de personnes.

7 - Système de sécurité conforme à la revendication 4, 5 ou 6, dans lequel le récepteur de compte (4) est un récepteur d'appel portable, un récepteur de table, une montre, un téléphone mobile, un ordinateur de téléphone général ou un dispositif électrique ou électronique spécialement conçu pour recevoir des signaux d'information d'action de transaction et afficher l'information d'action de transaction et a une unité d'alerte (4e) pour alerter le véritable possesseur concerné.

8 - Système de sécurité conforme à la revendication 4 ou 7, dans lequel la mémoire d'identification (4d) du récepteur de compte (4) a au moins un code d'identification ou un code d'adresse privé écrit par la station de transmission de signal d'action de transaction (3) et/ou des codes d'adresse supplémentaires tels qu'un code d'adresse (T) écrit par une compagnie de téléphone et/ou un code d'adresse (B) écrit par un système d'écriture de compte informatique de banque (2).

9 - Système de sécurité conforme à la revendication 4, dans lequel la station de transmission de signal d'action de transaction (3) envoie différents symboles d'affichage pour différentes actions de transactions telles qu'une action de transaction de cartes de crédit, une action de transaction de téléphone cellulaire, une action de transaction de téléphone à code secret, des nombres concernant la valeur monétaire de l'action de transaction, et des symboles et nombres et mots et caractères concernant le lieu de l'action de

transaction, le numéro de téléphone appelé et similaire.

10 - Système de sécurité conforme à la revendication 4, dans lequel sont prévus une pluralité de systèmes d'écriture de compte informatique (2) et de stations de transmission de signal d'action de transaction (3) qui peuvent être connectés dans un réseau afin que la zone de couverture de signal transmise par la station de transmission de signal d'action de transaction soit agrandie si nécessaire.

11 - Système de sécurité conforme à la revendication 4 ou 10, dans lequel un centre de traitement informatique de signal d'action de transaction (6) est prévu pour augmenter le nombre de signaux d'action de transaction et augmenter la vitesse de traitement.

12 - Procédé d'utilisation d'un système de sécurité conforme à l'une quelconque des revendications 1 à 11, pour informer immédiatement le véritable possesseur qu'une action de transaction de paiement monétique le concernant se produit, comprenant les étapes suivantes : pendant la durée d'une action de transaction transmettre une information concernant l'action de transaction au véritable possesseur, permettre au véritable possesseur de prendre une décision si l'action de transaction est autorisée ou non et informer le dispositif d'action de transaction (1) de la décision du véritable possesseur.

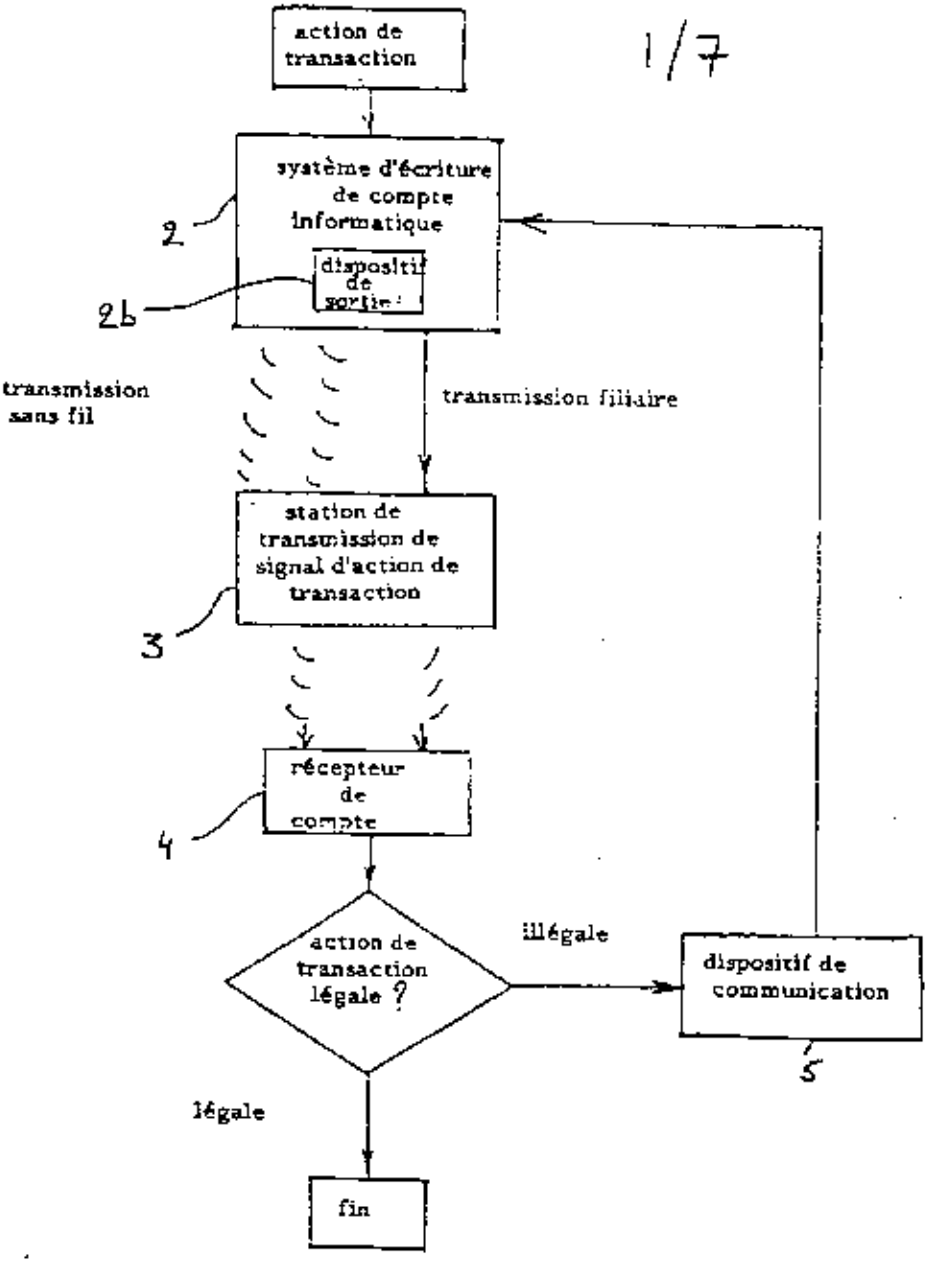

action de transaction
système d'écriture de compte informatique
2
dispositif de sortie
2b
transmission sans fil
transmission filiaire
station de transmission de signal d'action de transaction
3
récepteur de compte
4
action de transaction légale ?
illégale
dispositif de communication
5
légale
fin

Fig.1

2720176

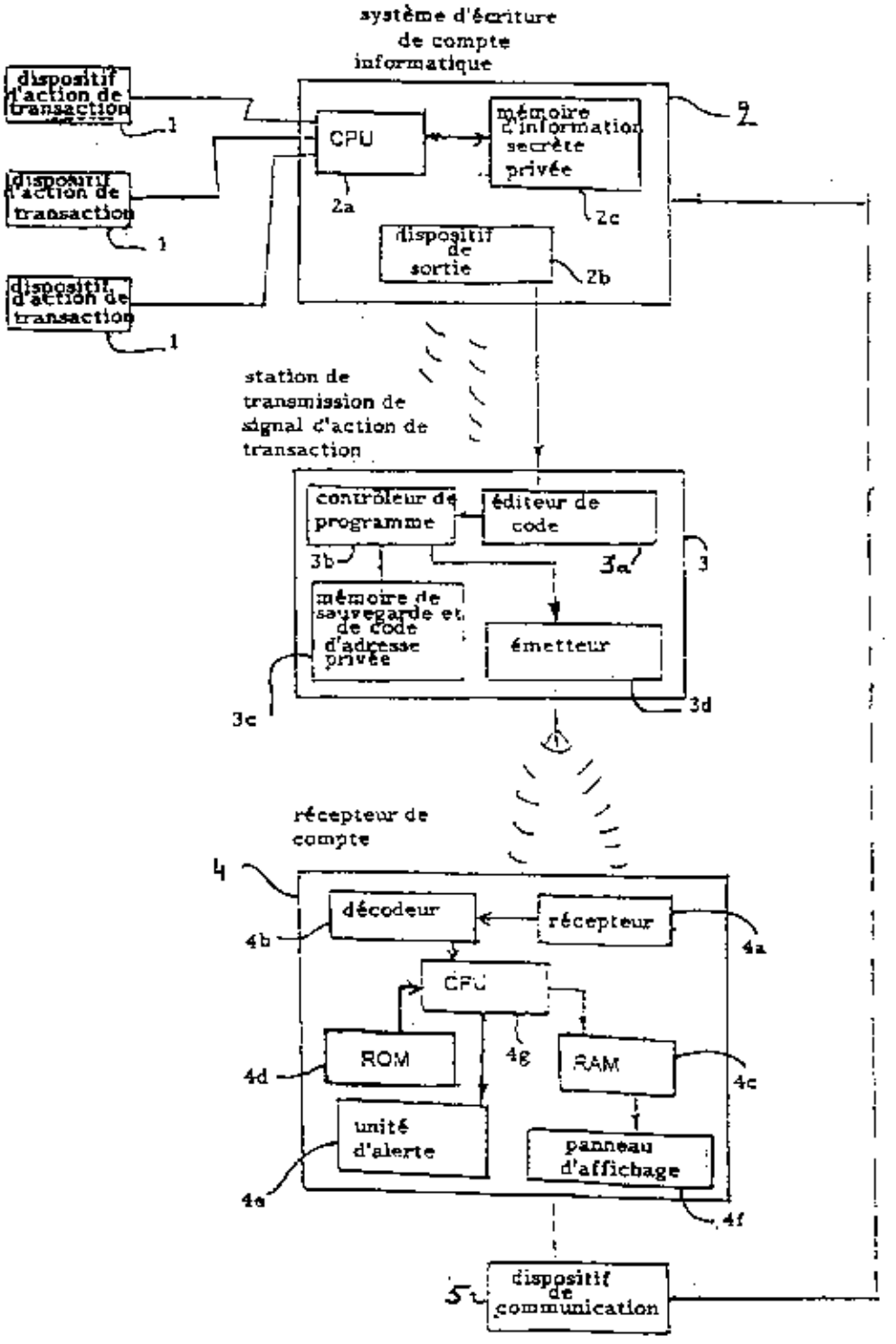


Fig.2

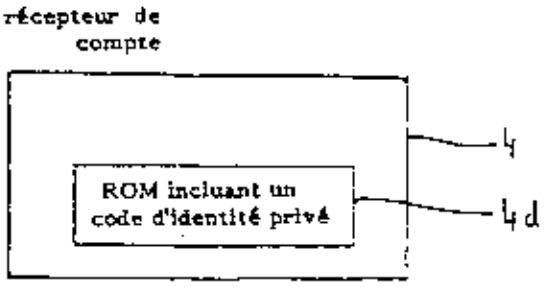

récepteur de compte
ROM incluant un code d'identité privé
4
4d

Fig.3-1

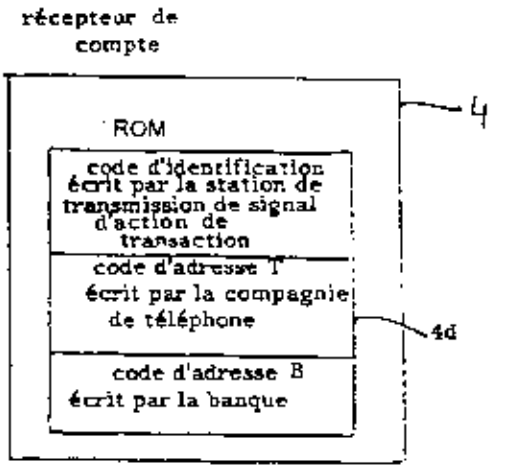

récepteur de compte
ROM
code d'identification écrit par la station de transmission de signal d'action de transaction
code d'adresse T écrit par la compagnie de téléphone
code d'adresse B écrit par la banque
4
4d

Fig.3-2

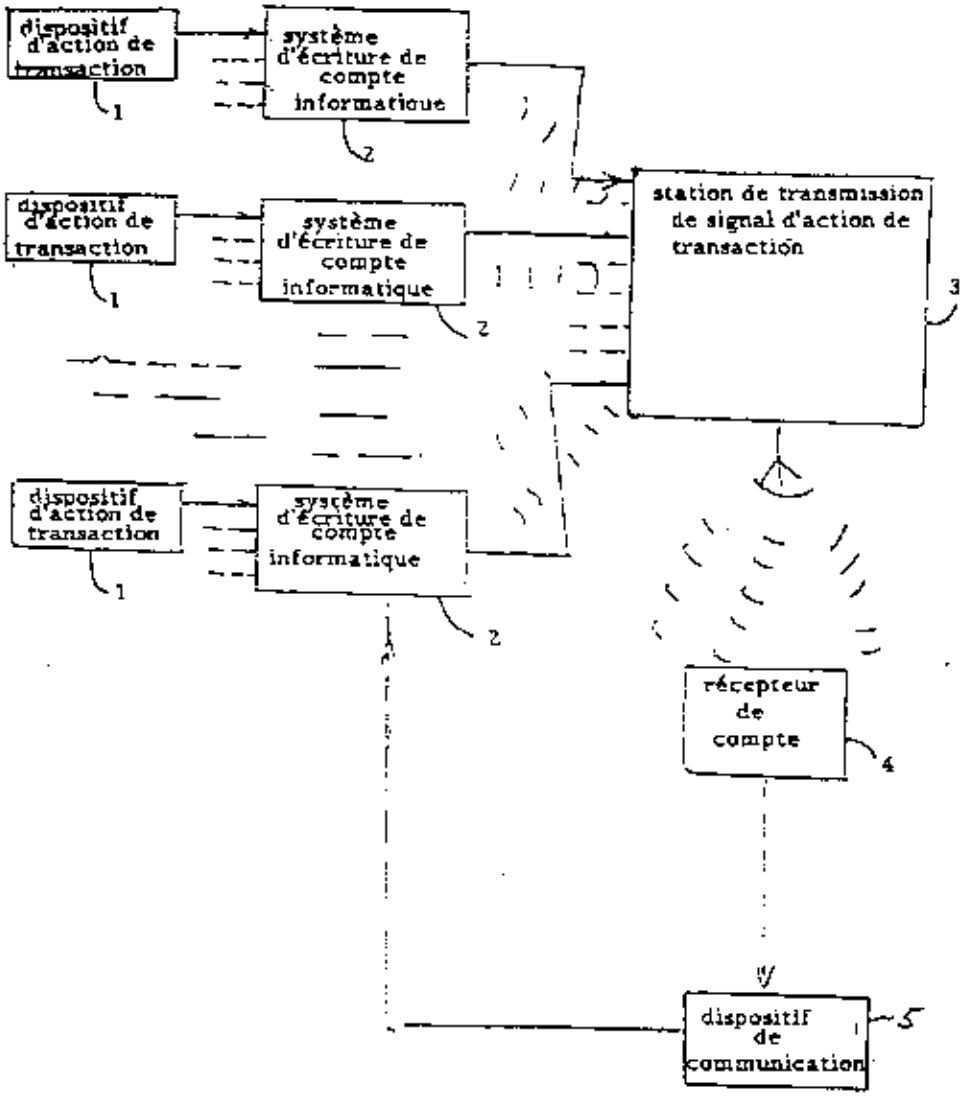

dispositif d'action de transaction
1
système d'écriture de compte informatique
2
dispositif d'action de transaction
1
système d'écriture de compte informatique
2
dispositif d'action de transaction
1
système d'écriture de compte informatique
2
station de transmission de signal d'action de transaction
3
récepteur de compte
4
dispositif de communication
5

Fig.4

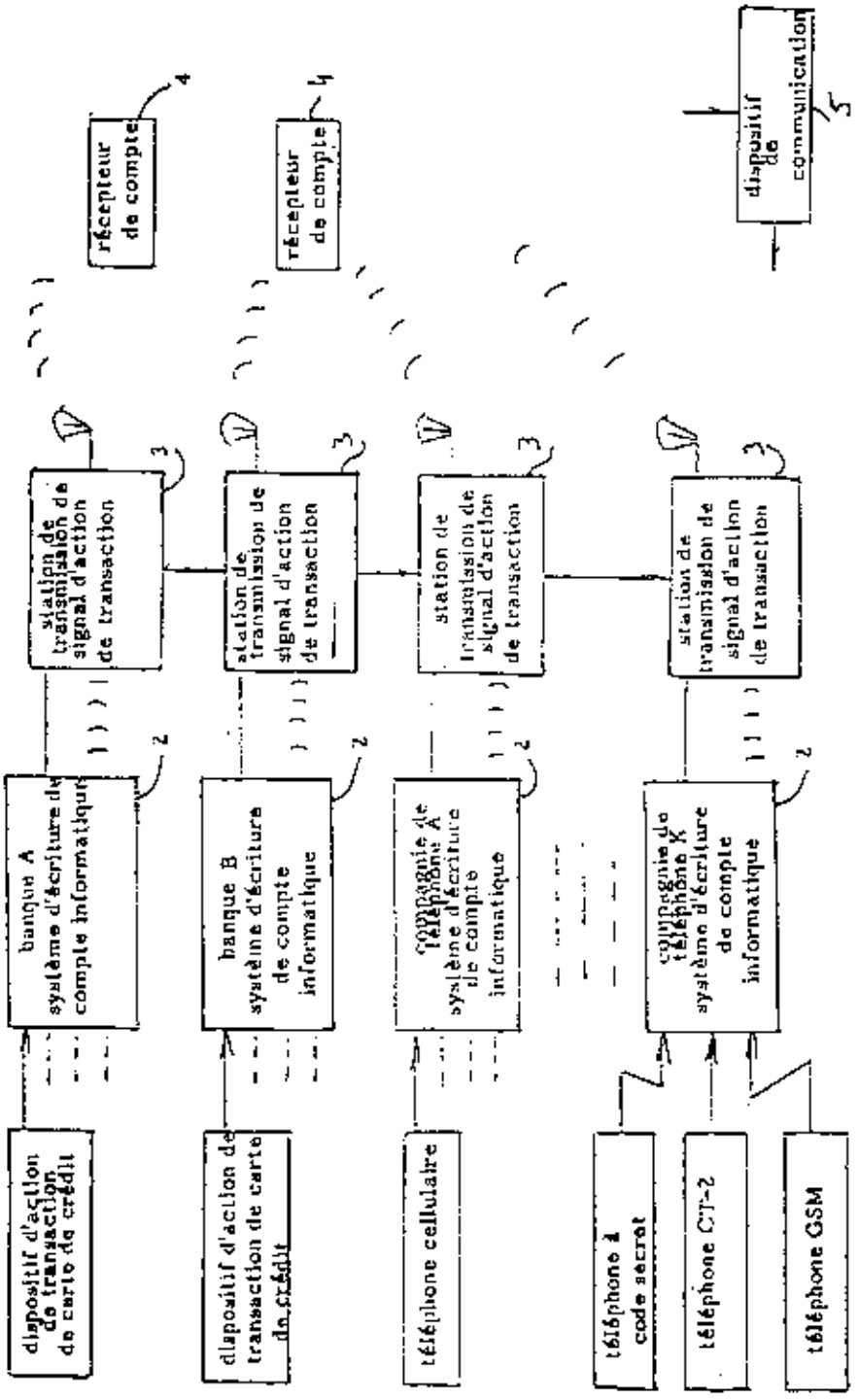

dispositif d'action de transaction de carte de crédit
banque A système d'écriture de compte informatique
station de transmission de signal d'action de transaction
récepteur de compte
dispositif d'action de transaction de carte de crédit
banque B système d'écriture de compte informatique
station de transmission de signal d'action de transaction
récepteur de compte
téléphone cellulaire
compagnie de téléphone A système d'écriture de compte informatique
station de transmission de signal d'action de transaction
téléphone à code secret
téléphone CT-2
téléphone GSM
compagnie de téléphone K système d'écriture de compte informatique
station de transmission de signal d'action de transaction
dispositif de communication

Fig.5

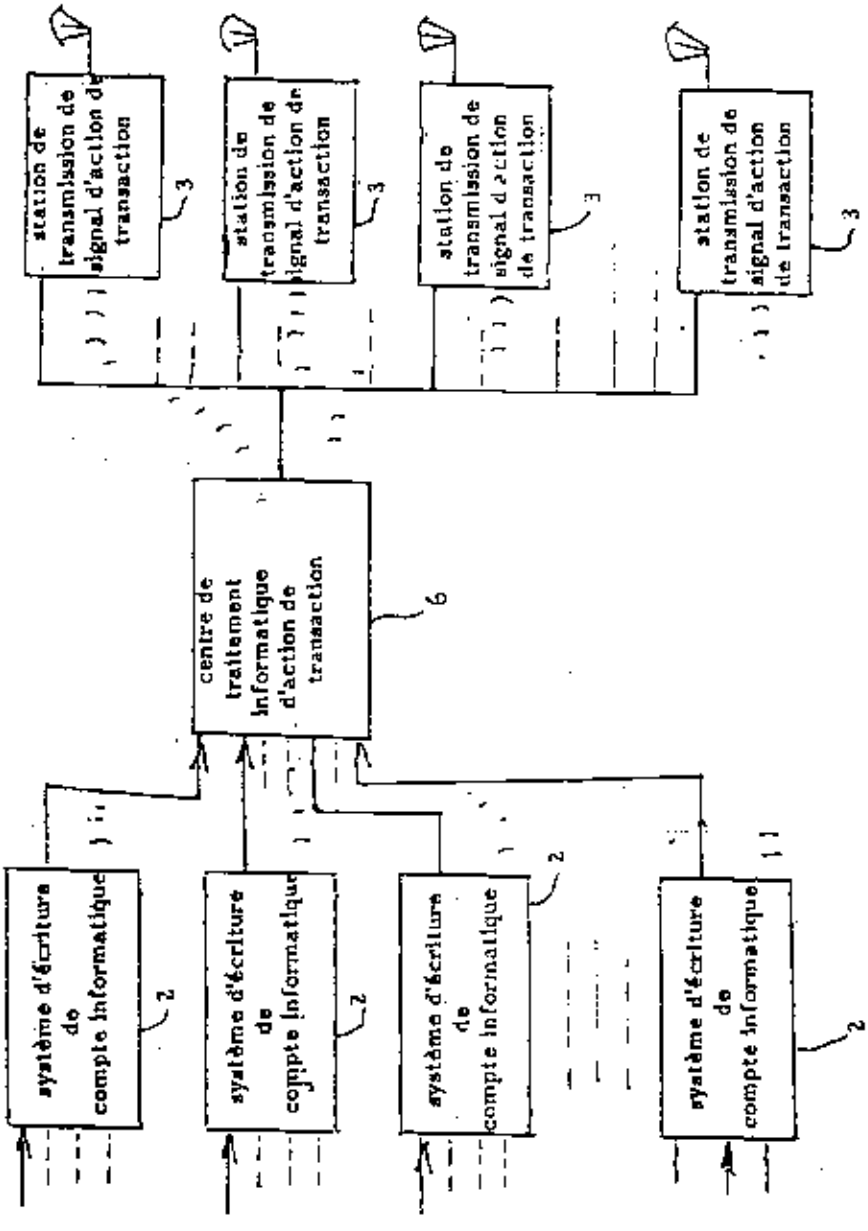

station de transmission de signal d'action de transaction
3
station de transmission de signal d'action de transaction
3
station de transmission de signal d'action de transaction
3
station de transmission de signal d'action de transaction
3
centre de traitement informatique d'action de transaction
6
système d'écriture de compte informatique
2
système d'écriture de compte informatique
2
système d'écriture de compte informatique
2
système d'écriture de compte informatique
2

Fig 8

7/7

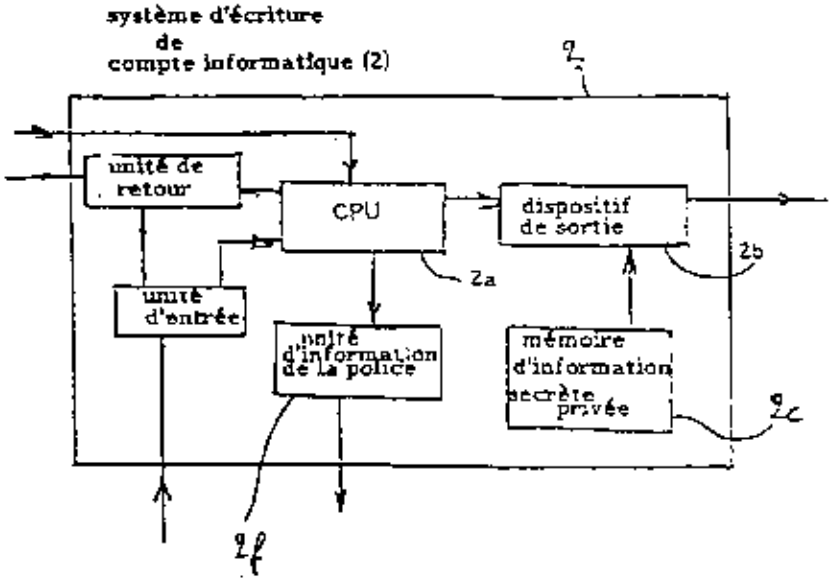

système d'écriture
de
compte informatique (2)
2
unité de
retour
CPU
dispositif
de sortie
2b
2a
unité
d'entrée
unité
d'information
de la police
mémoire
d'information
secrète
privée
2c
2f

Fig.7