

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication :  
(A n'utiliser que pour les  
commandes de reproduction).

**2 503 423**

A1

**DEMANDE  
DE BREVET D'INVENTION**

(21)

**N° 81 06396**

---

(54) Système de cartes à mémoire électronique pouvant être rechargées à des valeurs fiduciaires.

(51) Classification internationale (Int. Cl.<sup>3</sup>). G 06 K 19/00, 5/00, 7/00.

(22) Date de dépôt..... 31 mars 1981.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du  
public de la demande..... B.O.P.I. — « Listes » n° 40 du 8-10-1982.

---

(71) Déposant : FLONIC SA, résidant en France.

(72) Invention de : Pierre Bouvier.

(73) Titulaire : *Idem* (71)

(74) Mandataire : Henri Havre, Giers Schlumberger, service propriété industrielle,  
12, place des Etats-Unis, 92124 Montrouge.

Système de cartes à mémoire électronique pouvant être rechargées à des valeurs fiduciaires.

5

La présente invention est relative aux cartes à mémoire électronique, et notamment aux cartes de prépaiement auxquelles est attribuée initialement une certaine valeur fiduciaire, l'achat d'une carte moyennant le paiement de cette valeur permettant d'obtenir diverses prestations de service par annulations successives d'éléments de mémoire jusqu'à épuisement de sa valeur.

10

15

L'invention vise plus précisément un système de cartes dans lequel les cartes peuvent être rechargées à une valeur fiduciaire à la fin de leur utilisation sans risque de fraude.

20

On a déjà proposé pour l'obtention de prestations, par exemple de communications téléphoniques, d'utiliser une carte de prépaiement, cette carte présentant une piste magnétique sur laquelle sont enregistrés des signaux représentant des valeurs unitaires de prestations pour lesquelles la carte est utilisable. L'inconvénient de ce type de cartes est de présenter de trop grandes facilités de fraude en vue de leur restituer leur valeur initiale en prestations.

25

30

On connaît aussi des cartes à mémoire de type électronique utilisable pour le paiement de prestations dont la mémoire est constituée d'éléments fusibles qui

35

sont détruits progressivement au cours de l'utilisation de la carte. La valeur nominale de la carte, c'est-à-dire le nombre des unités de paiement à la disposition de l'utilisateur, est proportionnelle au nombre d'éléments ou cellules de la mémoire, généralement de type matriciel, l'un des deux états possibles dans lequel se trouve cet élément correspondant à une valeur fiduciaire conventionnelle.

10

Une telle carte, après épuisement de sa valeur nominale, n'est plus utilisable en tant que support de valeur fiduciaire puisque les éléments de sa mémoire électronique une fois détruits, celle-ci n'est plus "rechargeable" à sa valeur initiale. La carte doit alors être jetée, ce qui, par suite, oblige à limiter sa valeur intrinsèque à un minimum et donc la capacité de sa mémoire si on ne veut pas que son prix représente un trop fort pourcentage des prestations qu'elle peut fournir.

20

On connaît encore des cartes à mémoire électronique utilisables comme cartes de paiement à crédit variable mis à jour au prorata des paiements effectués, par exemple du genre décrit dans les brevets français N° 2.266.222, 2.304.992, 2.304.989, 2.311.365.

25

Cependant, des dispositions sont normalement prévues dans ce genre de cartes pour interdire leur recharge ; par suite, leur prix intrinsèque représente encore un trop fort pourcentage vis-à-vis de la valeur fiduciaire en prestations qui leur est attribuée.

35

L'invention vise un système de cartes à mémoire non volatile pour le paiement de prestations, le système étant prévu pour permettre de recharger les cartes après épuisement de leur valeur fiduciaire tout en assurant une bonne protection contre les risques de fraude.

Le fait d'utiliser une mémoire rechargeable a en effet l'inconvénient d'ouvrir la possibilité aux tentatives de fraude en vue de pratiquer cette opération de rechargement de la mémoire de façon illicite.

L'invention propose plus particulièrement un système de cartes du genre exposé précédemment dans lequel des dispositifs en vue de protéger les cartes contre un rechargement frauduleux exécuté par une personne non habilitée et/ou dehors de machines de rechargement adaptées pour n'effectuer cette fonction que sur des cartes appropriées.

Suivant l'invention, la carte comporte :

25

- une mémoire électronique non volatile comprenant :

30

. une zone transactionnelle d'éléments de mémoire initialement mis dans un état déterminé,

. une deuxième zone inscriptible une seule fois, dans laquelle est mémorisé un numéro d'identification accessible à la lecture ; et

35

- 4 -

. une troisième zone, inscriptible une seule fois,  
dans laquelle est mémorisé un nombre clé  
inaccessible à la lecture ;

5 et

- un circuit comparateur ayant une première entrée  
reliée à ladite troisième zone et une seconde  
entrée branchée pour recevoir un nombre déduit par  
10 un algorithme du numéro d'identification lu dans la  
deuxième zone, et sa sortie reliée à une porte de  
commande d'écriture dans ladite zone  
transactionnelle pour y appliquer un signal de  
validation quand l'identité du nombre clé et du  
15 nombre déduit par algorithme est vérifiée par le  
comparateur,

et elle est caractérisée en ce que ladite zone  
transactionnelle de mémoire est effaçable à travers  
20 ladite porte de commande d'écriture et réinscriptible.

Ainsi, le numéro d'identification et le nombre clé ne  
pouvant plus être modifiés, seule la connaissance de  
25 l'algorithme permet de déduire du numéro  
d'identification (accessible à la lecture), le nombre  
clé (secret), et par conséquent de valider la porte de  
commande d'écriture autorisant l'effacement de la zone  
transactionnelle de la mémoire. Une protection efficace  
30 contre les tentatives de rechargement frauduleux de la  
carte est alors assurée en choisissant un nombre clé  
suffisamment long pour exclure toute déduction qui  
serait l'effet du hasard.

35

La carte à mémoire selon l'invention, assure donc les mêmes fonctions que celles qui ont été décrites précédemment, mais utilisant une mémoire d'un type susceptible d'être rechargée, par exemple à stockage de charges électriques, une réutilisation de la même carte après un premier épuisement de sa valeur fiduciaire est ainsi rendu possible à plusieurs reprises. Le rétablissement de sa valeur nominale (ou d'une valeur différente) est obtenu grâce à un "rechargement" de la zone transactionnelle de sa mémoire, bien entendu contre un paiement correspondant comme lors de son achat initial.

Dans la suite de cet exposé, on utilisera le terme "chargement" ou "rechargement" pour signifier la remise des éléments de mémoire dans leur état initial prédéterminé auquel est attribué conventionnellement une valeur fiduciaire, quelle que soit la technologie de la mémoire utilisée.

Le rechargement ou effacement sélectif de la zone transactionnelle de mémoire déjà inscrite peut être réalisé de façons différentes selon le type choisi pour la mémoire de la carte. Dans le cas d'une mémoire de type EAROM, mémoire morte électriquement altérable, par exemple en technologie MNOS ou DIFMOS, l'effacement est obtenu électriquement par adressage successif des cellules inscrites, les deuxième et troisième zones étant protégées contre une réécriture par un élément à changement d'état irréversible bloquant définitivement une porte d'écriture dans ces zones.

5      Accessoirement, il est aussi prévu de faire comporter à la mémoire, dans la zone transactionnelle, une série de cellules servant de registre dans lequel est inscrit le montant de la valeur fiduciaire chargée initialement, ou rechargée, dans la carte lors de son achat, ou de sa recharge.

10      L'invention prévoit aussi des machines fonctionnant en coopération avec la carte précédente, soit comme machine de chargement (ou de rechargement) lors d'une phase initiale d'achat de prestations introduisant un "crédit" dans la carte, soit comme machine d'inscription de "débit" dans la carte lors d'une phase de paiement d'une prestation, par exemple une communication téléphonique.

20      La machine d'effacement (ou de chargement) comporte des moyens de lecture des zones accessibles de la mémoire de la carte, un circuit cryptographique, fonctionnant suivant l'algorithme reliant le numéro d'identification et le nombre clé et ayant son entrée pouvant être reliée à la deuxième zone de la mémoire de la carte et sa sortie reliée à la seconde entrée du comparateur de la carte, et des moyens d'écriture prévus pour être reliés à la porte de commande d'écriture de la carte pour mettre les éléments de la zone transactionnelle de la mémoire dans leur état initialement déterminé.

30

La machine d'inscription de débits fonctionnant en coopération avec la carte de prépaiement comporte de

35

préférence un opérateur logique effectuant  
préalablement à l'autorisation de toute prestation, une  
vérification du solde restant dans la carte en  
retranchant du crédit effectif trouvé dans la carte par  
5 lecture du registre prévu à cet effet la somme des  
débits inscrits depuis son dernier chargement. Le  
résultat de cette soustraction, s'il est positif, donne  
à la machine l'autorisation d'entamer le processus de  
la prestation. Si au contraire le résultat est nul, il  
10 provoque l'émission d'un signal d'arrêt interdisant à  
la machine d'effectuer la prestation.

Dans une version simple, à chaque élément de mémoire de  
15 la zone transactionnelle est affectée une valeur  
monétaire fixe ; dans une version plus élaborée, la  
mémoire de la zone transactionnelle est découpée en  
groupe d'éléments représentant respectivement une  
valeur monétaire fixe, chaque groupe comprenant  
20 plusieurs éléments de poids binaires croissants et un  
élément de bit de parité.

La carte suivant l'invention possédant la propriété  
25 d'être rechargeable sous la condition de sécurité  
énoncée plus haut, elle peut subir un certain nombre de  
cycles d'inscription-effacement avant que sa mémoire  
perde ses qualités de mémorisation correcte à la suite  
du phénomène de fatigue obligeant à la mettre hors de  
30 service. Il est alors concevable que, bien que sa  
valeur intrinsèque, c'est-à-dire son prix de revient,  
puisse paraître à première vue assez élevé en raison de  
sa circuiterie élaborée, elle est en réalité amortie



sur une somme importante (valeur fiduciaire x nombre de recharges) vis-à-vis de laquelle ce prix de revient représente finalement un pourcentage très faible.

5

Les prestations de service qu'une telle carte utilisable comme carte de prépaiement, peut permettre d'obtenir ne sont naturellement pas limitées aux communications téléphoniques, citées plus haut à titre d'exemple, mais peuvent s'étendre à des services divers : péage de transport, d'autoroute, de stationnement ; distribution d'objets, etc ... Bien entendu, une telle carte est aussi utilisable comme carte de paiement ou comme carte de crédit, la valeur fiduciaire initiale ou le montant du crédit étant inscrit dans le registre à cet effet, et les débits successifs inscrits dans le reste de la zone transactionnelle jusqu'à épuisement de cette valeur ou de ce montant.

20

D'autres caractéristiques et avantages de l'invention ressortiront de la description suivante et du dessin annexé, donné à titre d'exemples non limitatifs de mise en oeuvre de systèmes de cartes suivant l'invention. Sur ce dessin :

25

- la fig. 1 représente un schéma synoptique expliquant le principe de chargement d'une carte conforme à l'invention.

30

- la fig. 2 représente schématiquement un système à carte de prépaiement plus élaborée conforme à l'invention.

35

Dans les exemples qui vont suivre, on supposera, pour fixer les idées, que la zone transactionnelle des débits dans la carte est "chargée" quand ses éléments sont à l'état ou au niveau logique 0 et que la mise à l'état ou au niveau logique 1 d'un élément indique que la valeur fiduciaire correspondant à cet élément de mémoire a été dépensée et est donc nulle.

10 Sur la fig. 1, on a représenté schématiquement le circuit électronique 10 d'une carte qui comporte essentiellement : un circuit d'interface (non représenté) relié à des contacts permettant le raccordement électrique de ce circuit à une machine, dite machine de transfert de données ; une mémoire 11 ; un circuit comparateur numérique 12 et une porte d'écriture 13 ayant une entrée de validation reliée à la sortie du comparateur 12.

20 La mémoire 11 est une mémoire non volatile de type effaçable et réinscriptible, par exemple à stockage de charges électriques arrangées suivant un mode matriciel. La mémoire 11 est divisée en trois zones 25 111, 112, 113. La zone 111, dite zone de mémoire transactionnelle et réservée à l'inscription des débits, est toujours accessible à la lecture, mais l'écriture n'y est possible que sous condition, comme il sera expliqué plus loin, et en particulier son effacement n'est possible qu'à travers la porte 30 d'écriture 13. La zone 112, destinée à mémoriser un numéro d'identification propre à chaque carte, est toujours accessible à la lecture, mais elle n'est

35

5 inscriptible qu'une seule fois dans une phase d'initialisation de la carte, et son entrée d'écriture est ensuite interdite par le changement d'état irréversible d'un élément, tel qu'une rupture de fusible bloquant définitivement une porte d'écriture dans cette zone.

10 La zone 113, destinée à renfermer un nombre clé est inscriptible une seule fois au cours de la phase d'initialisation et ensuite protégée par exemple par rupture de fusible ; de plus, elle n'est pas accessible à la lecture de l'extérieur de la carte, mais seulement  
15 reliée à l'une des entrées du comparateur 12. Il existe une relation entre le nombre d'identification et le nombre clé respectivement inscrits dans les zones 112 et 113, cette relation résultant d'un algorithme de sécurité.

20 L'alimentation électrique du circuit 10 est assurée quand la carte est accouplée à la machine de transfert par une source contenue dans cette dernière, à travers des contacts ou éventuellement par voie  
25 électromagnétique, inductive ou optique, à cet effet.

La machine de transfert de données 20 comprend de son côté : un circuit cryptographique 21 ayant une entrée  
30 pouvant être reliée à la sortie de la zone 112 de la mémoire 11 de la carte et une sortie pouvant être reliée à la seconde entrée du comparateur 12 quand la carte est accouplée à la machine 20 ; un circuit de

35

- 11 -

5 commande d'écriture 22, équipé d'un clavier, a sa sortie pouvant être connectée à une seconde entrée de la porte d'écriture 13 de la carte ; un circuit de commande à programme 23 renfermant un circuit générateur de signaux d'horloge H pilote l'ensemble des opérations de lecture et d'écriture dans la carte.

10 Bien entendu, le circuit cryptographique 21 utilise l'algorithme traduisant la relation entre le nombre d'identification et le nombre clé qui ont été inscrits respectivement dans les zones de mémoire 112 et 113 de la carte.

15 A la suite de la phase d'initialisation au cours de laquelle les zones de mémoire 112 et 113 ont été chargées et protégées comme il a été expliqué plus haut, la carte est chargée à une valeur déterminée  
20 correspondant à un nombre N de prestations, en supposant dans cet exemple que chaque élément de mémoire représente une valeur unitaire de prestation pour laquelle la carte est utilisable. Pour ce faire, la carte est accouplée à la machine 20 et la commande  
25 programmée 21 provoque en premier lieu la lecture de la zone 112 de la mémoire 11 de la carte. Une première série de signaux représentant le nombre d'identification lu en 112, est alors convertie par le circuit de cryptage 21 en une autre série de signaux  
30 qui sont envoyés sur la seconde entrée du comparateur 12 de la carte, la première entrée recevant les signaux de lecture du nombre clé inscrit dans la zone 113.

35

L'identité des deux séries de signaux, résultant de la vérification de la relation entre nombre clé et nombre d'identification, a pour effet que le comparateur fournit sur la porte 13 un signal de validation. Il est  
5 alors possible, et seulement si cette vérification a été faite, au moyen de circuit d'écriture 22 d'accéder à la zone 113 de la mémoire 11 pour y porter au niveau logique 0 le nombre N d'éléments correspondant à la valeur fiduciaire que la carte est destinée à  
10 représenter.

Dans le cas d'une carte déjà utilisée et que l'on désire recharger, le processus se déroule de façon  
15 analogue par remise à zéro d'éléments en nombre correspondant à la valeur fiduciaire attribuée à la carte.

20 Il est facile de voir que toute tentative de fraude pour écrire des zéros dans la zone de mémoire transactionnelle 113 est impossible sans connaître la relation entre les deux nombres définitivement mémorisés dans les zones de mémoire 112 et 113, l'un  
25 d'eux étant par ailleurs inaccessible à la lecture extérieure.

L'algorithme traduisant cette relation pouvant faire  
30 appel à des nombres aléatoires ou pseudo-aléatoires, il est pratiquement impossible à un fraudeur de découvrir cette relation. Une très grande sécurité est ainsi garantie contre les tentatives frauduleuses pour recharger une carte conforme à l'invention.

35

Le principe de chargement d'une carte ayant été ainsi exposé, on va maintenant décrire plus en détail le mode de fonctionnement d'un système de cartes à mémoire rechargeable dans lequel la zone de mémoire rechargeable est organisée en groupes ou section d'éléments, chaque groupe représentant respectivement une valeur fiduciaire déterminée et contenant un certain nombre d'éléments de mémoire de poids binaires croissants plus un bit de parité. Un tel système est schématisé à la fig. 2.

La carte 30 comporte : une mémoire 31 associée à un compteur d'adresse 32 et à un décodeur d'adresse 33, une logique d'écriture 34 reliée à la sortie du décodeur 31 et commandant des portes d'écriture de 1 et de 0 respectivement, et un circuit d'interface 35 pouvant recevoir les signaux issus d'une machine d'inscription de débit 40 (ou d'une machine de transfert de données) et lui transmettant des signaux de lecture de la mémoire 31.

Bien entendu, la carte comporte aussi comme sur la fig. 1, un circuit comparateur relié à la zone de mémoire 313 définie ci-après, ainsi qu'une porte d'écriture validable par ce comparateur, ces éléments n'ayant pas été représentés pour ne pas surcharger la figure.

La mémoire 31 comprend : d'une part, des données mémorisées définitivement et protégées contre une modification de leur contenu par exemple par rupture de

5 fusible ; il s'agit, dans les zones 311 et 312,  
toujours accessibles à la lecture, du nombre  
d'identification de la carte et d'un code  
caractéristique de ou des prestations que la carte  
10 permet d'obtenir, et dans la zone 313, non accessible à  
la lecture extérieure mais reliée au comparateur, du  
nombre clé de la carte ; d'autre part des données  
pouvant être inscrites et effacées sous conditions dans  
une zone transactionnelle 314, comportant en  
particulier un registre 315 destiné à enregistrer le  
montant initial de chargement de la carte, autrement  
dit sa valeur fiduciaire initiale avant inscription de  
tout débit.

15

Contrairement aux autres données de débit mémorisées  
dans le reste de la zone de mémoire 314, les données  
contenues dans le registre 315 sont inscrites en  
complémentaire par rapport à ces autres données,  
20 c'est-à-dire, suivant une convention inverse de celle  
que l'on a adoptée exemplairement à l'origine, que dans  
ce registre 315 le niveau logique 1 représente une  
charge et le niveau 0 une valeur nulle.

25

La zone de mémoire effaçable 314 est divisée en groupe  
d'éléments unitaires de mémoire GE de poids binaires  
croissants associés respectivement à un bit de parité,  
par exemple en octets comprenant 7 bits de valeur + 1  
30 bit de parité. A chaque groupe d'éléments GE est  
attribuée une valeur fiduciaire préétablie, par exemple  
 $2^7 = 1,28$  Franc, 1 centime pour le bit de rang 1, 2  
centimes pour le bit de rang 2, et ainsi de suite, et

35

il est, en outre, prévu que tout groupe d'éléments GE inscrit partiellement ou totalement n'est plus ensuite modifiable en écriture.

5

Le compteur d'adresse 32 permet en coopération avec le décodeur 33 d'explorer séquentiellement la mémoire 31 préalablement à toute opération de chargement de la carte ou d'inscription d'un débit relatif à une prestation.

10

La logique 34 comporte des portes d'écriture notamment la porte (13, fig. 1) commandée par le comparateur (12, fig. 1) utilisée lors d'une opération de chargement de la carte; ainsi que d'autres portes commandées par le décodeur d'adresse 33 de façon telle que, avec la convention adoptée :

15

20 - l'inscription d'un 1 (correspondant à un débit) dans la zone transactionnelle 314 est toujours possible, sauf dans le registre 315 (ici correspondant à un crédit) où cette inscription est conditionnée par la sortie du comparateur ;

25

- l'inscription d'un 0 (correspondant à un crédit) dans la zone transactionnelle 314 est conditionnée par la sortie du comparateur, sauf dans le registre 315 (correspondant à un débit) où une telle inscription est toujours possible.

30

La machine d'inscription de débits 40 comprend un mécanisme récepteur de carte d'un type quelconque (non

35



représenté), un circuit de commande à programme 41  
associé à un générateur de signaux d'horloge H, un  
opérateur numérique 42 permettant de vérifier que la  
différence du montant de chargement initial de la carte  
5 avec la somme des débits inscrits dans la zone  
transactionnelle 314 de la carte 30 est bien positive,  
un circuit d'écriture 43 et une porte d'écriture 44.  
Les signaux de lecture S de la zone de mémoire 314 de  
la carte à travers le circuit d'interface 35 sont  
10 appliqués sur les circuits 41 et 42. Ce dernier fournit  
deux signaux suivant que la différence calculée est  
positive ou nulle, l'un de ces signaux étant appliqué  
sur la machine prestataire M, par exemple une  
installation téléphonique, soit pour autoriser la  
15 prestation dans la limite du solde créditeur restant  
dans la carte, soit pour interdire la mise en route ou  
la poursuite de la prestation si le solde créditeur  
dans la carte est nul ou devient inférieur à un seuil  
déterminé. Eventuellement, la machine peut encore  
20 comporter un dispositif d'affichage 45 de ce solde  
restant.

La machine prestataire M est agencée pour fournir au  
25 circuit d'écriture 43 des signaux en nombre  
proportionnel ou fonction de la prestation fournie à  
l'utilisateur de la carte.

30 La commande à programme 41 est conçue pour fournir des  
signaux C qui, en combinaison avec les signaux E issus  
de la porte 44 sont interprétés par le circuit  
d'interface 35 de la carte 30 suivant quatre types  
d'ordre:

35

- 17 -

- remise à zéro du compteur d'adresse 32,
  - avance d'un pas du compteur d'adresse 32,
  - 5 - écriture d'un 0,
  - écriture d'un 1,
- 10 l'ensemble des opérations étant cadencé par les signaux d'horloge H.

Le fonctionnement de ce système est le suivant au cours de l'obtention d'une prestation de service :

15 La carte 30 étant accouplée à la machine 40 et les contacts électriques établis entre ces deux éléments, la commande à programme 41 entame le processus par un ordre de lecture de la zone 312 de la mémoire de la

20 carte contenant le code de service caractéristique afin de vérifier en premier lieu que la carte 30 correspond bien au type de la machine dans laquelle elle a été introduite et/ou donne droit à la prestation désirée ; l'emplacement de ce code étant le même dans toutes les

25 cartes, l'adressage de la zone 312 peut être fait sans ambiguïté. Si le code lu correspond au code caractéristique, la commande 41 autorise la poursuite du processus. Dans le cas contraire, un signal d'arrêt est émis par la commande qui interdit cette poursuite,

30 et la carte est restituée à l'utilisateur.

35

Le processus se poursuit alors par lecture systématique de la mémoire transactionnelle 314 en commençant par le montant de la charge initiale de la carte mémorisée dans le registre 315, puis des débits inscrits dans les différents groupes d'éléments unitaires GE jusqu'à 5 détection du premier groupe GE vierge n'ayant donné lieu à aucune inscription de débit. Les signaux de lecture S obtenus sont traités dans le circuit opératoire 42 qui établit le solde restant dans la 10 carte. Si ce solde est nul ou inférieur au seuil déterminé, par exemple le tarif unitaire de la prestation désirée, le signal d'arrêt est émis par le circuit 42 et la carte restituée. En revanche, si ce solde est suffisant, le circuit 42 autorise le 15 démarrage de la prestation, par exemple une communication téléphonique. Les impulsions correspondantes fournies (pour chaque unité tarifaire) par la machine prestataire M sont appliquées sur le circuit d'écriture 43 qui les convertit en impulsions 20 représentatives d'argent. Celles-ci, à travers la porte 44 validée par le circuit 42 sont inscrites dans le premier groupe GE vierge de la zone de mémoire 314 de la carte, et dans le ou les suivants si nécessaire en cas de report. Après chaque inscription, la zone de 25 mémoire 314 est explorée et le solde restant mis à jour, la prestation étant interrompue si le crédit restant dans la carte vient à être épuisé ou devient inférieur à une unité tarifaire au cours de son déroulement. En fin de prestation, la carte est 30 restituée à l'utilisateur.

Le rechargement d'une carte de ce type à une valeur préétablie est effectué selon le principe exposé à la fig. 1. Dans le cas d'une carte où chaque élément de mémoire de la zone transactionnelle possède la même valeur fiduciaire fixe, la machine d'effacement est conforme au schéma indiqué à la fig. 1.

Dans le cas d'une carte du genre représenté à la fig. 2 où la mémoire transactionnelle est divisée en groupes d'élément GE, la machine d'effacement doit être équipée d'un circuit opératoire et d'un organe d'affichage, analogue aux éléments 42 et 45 de la fig. 2, afin de pouvoir évaluer le solde éventuel restant dans la carte par différence entre la valeur inscrite dans le registre 315 et la somme des débits inscrits dans le reste de la zone 314. Le processus de chargement est alors le suivant : après vérification initiale de la relation entre numéro d'identification et nombre clé aboutissant, si cette condition de sécurité est vérifiée, au déblocage de la porte de commande d'écriture (13, fig. 1), la machine procède à la lecture de la zone transactionnelle et affiche le solde trouvé dans la carte. Un circuit d'écriture équipé d'un clavier permet alors à travers la porte débloquée comme ci-dessus :

- a) d'effacer en totalité la zone 314 par adressages successifs de ses éléments, c'est-à-dire de ramener à leur niveau logique initial 0 tous les éléments de cette zone, y compris ceux du registre 315 ;

- 20 -

b) d'inscrire dans le registre 315 le montant de la valeur fiduciaire que l'on désire attribuer à la carte, l'écriture de ce montant étant réalisée en code complémentaire, suivant lequel c'est le niveau  
5 logique 1 qui représente une charge et le niveau logique 0 une valeur nulle. Ce montant est, par exemple pour une carte à prépaiement, égal à la somme payée par le possesseur de la carte augmentée du solde restant avant effacement.

10

Il est à remarquer que dans cette opération de chargement, tous les éléments de mémoire de la zone transactionnelle extérieure au registre 315,  
15 c'est-à-dire destinée à l'enregistrement des débits, sont amenés à un même état initial et que la valeur fiduciaire théorique contenue dans cette zone peut être largement supérieure à la valeur mémorisée dans le registre 315. Cela tient au fait qu'on a choisi, pour  
20 simplifier les circuits, de ne plus écrire dans les groupes d'éléments unitaires GE déjà partiellement inscrits, ce qui par suite nécessite un plus grand nombre de groupes d'éléments GE que le nombre strict correspondant exactement à la valeur "faciale" de la  
25 carte. En réalité, il n'en résulte aucune erreur du point de vue comptable puisque c'est la valeur inscrite dans le registre 315, correspondant à la somme réellement déboursée par le possesseur de la carte, qui sert de référence pour le calcul du solde créditeur.

30

Bien entendu des modifications peuvent être apportées au système qui vient d'être décrit à titre d'exemple

35

- 21 -

sans sortir du domaine de l'invention. De plus, la  
carte n'est pas exclusivement utilisable comme carte à  
prépaiement, mais peut aussi bien être utilisée comme  
carte de paiement et carte de crédit, le montant du  
5 crédit et les débits successifs étant inscrits  
respectivement dans le registre et le reste de la zone  
de mémoire transactionnelle.

10

15

20

25

30

35

REVENDEICATIONS

- 1 - Carte utilisable pour le paiement de prestations individuelles par changement d'état d'éléments de mémoire et comportant :
- 5
- une mémoire électronique non volatile comprenant :
- 10
- . une zone transactionnelle d'éléments de mémoire initialement mis dans un état déterminé,
  - . une deuxième zone inscriptible une seule fois, dans laquelle est mémorisé un numéro

15

  - d'identification accessible à la lecture ; et
  - . une troisième zone, inscriptible une seule fois, dans laquelle est mémorisé un nombre clé

20

  - inaccessible à la lecture ;
- et
- un circuit comparateur ayant une première entrée reliée à ladite troisième zone et une seconde
- 25
- entrée branchée pour recevoir un nombre déduit par un algorithme du numéro d'identification lu dans la deuxième zone, et sa sortie reliée à une porte de commande d'écriture dans ladite zone transactionnelle pour y appliquer un signal de
- 30
- validation quand l'identité du nombre clé et du nombre déduit par algorithme est vérifiée par le comparateur,
- 35

- 23 -

Carte caractérisée en ce que ladite zone transactionnelle de mémoire (111,314) est effaçable à travers ladite porte de commande d'écriture (13) et réinscriptible.

5

2 - Carte suivant la revendication 1 dans laquelle la mémoire est réalisée en technologie à effacement électrique, caractérisée en ce que l'effacement est obtenu par adressage successif des éléments de mémoire inscrits.

10

3 - Carte suivant la revendication 2, caractérisée en ce que lesdites deuxième (112;311) et troisième (113;313) zones de mémoire sont protégées contre une réécriture par un élément à changement d'état irréversible bloquant définitivement une porte d'écriture dans ces zones.

15

20

4 - Carte suivant l'une des revendications précédentes, caractérisée en ce que, dans la zone transactionnelle (314) de la mémoire (31), est prévu un registre (315) destiné à mémoriser une valeur fiduciaire initiale inscrite en complémentaire par rapport aux inscriptions dans le reste de ladite zone transactionnelle.

25

30

5 - Carte suivant la revendication 4, caractérisée en ce que la zone transactionnelle (314) de mémoire extérieure audit registre (315) est divisée en

35



groupes d'éléments unitaires de mémoire (GE) de poids binaires croissants, chaque groupe d'éléments (GE) dans un état initial déterminé représentant une valeur fiduciaire préétablie.

5

6 - Carte suivant la revendication 5, caractérisée en ce qu'à chacun desdits groupes d'éléments (GE) est associé un bit de parité.

10

7 - Carte suivant la revendication 4, caractérisée en ce qu'elle comporte une logique d'écriture reliée à la sortie du circuit comparateur et prévue pour autoriser la remise à leur état initial déterminé des éléments de mémoire de la zone transactionnelle et la mise à l'état complémentaire de cet état initial d'éléments dudit registre seulement si le signal de validation est reçu du circuit comparateur.

15  
20

8 - Machine d'inscription de débits dans une carte, suivant les revendications 4 et 5, comportant des moyens de lecture de la zone transactionnelle de la carte quand celle-ci est connectée à la machine, un circuit d'écriture ayant sa sortie reliée à une porte d'écriture, caractérisée en ce qu'elle comporte, en outre, un circuit opérateur numérique (42) effectuant la différence entre la valeur fiduciaire lue dans le registre (315) de la zone de mémoire transactionnelle (314) et la somme des

25

30

35

5 valeurs fiduciaires représentées par les éléments  
de mémoire dont l'état a été changé dans chaque  
groupe d'éléments (GE), ledit circuit opérateur  
fournissant un signal provoquant respectivement le  
déblocage de ladite porte d'écriture (44) quand  
cette différence est positive et provoquant le  
blocage de ladite porte et l'arrêt de la machine  
quand cette différence est inférieure à une valeur  
de seuil déterminée.

10

9 - Machine d'effacement d'une carte, suivant la reven-  
dication 1, comportant des moyens de lecture des  
zones accessibles de la mémoire de la carte quand  
celle-ci est connectée à la machine, un circuit  
15 cryptographique fonctionnant suivant ledit  
algorithme et ayant son entrée pouvant être reliée  
à la deuxième zone de la mémoire de la carte et sa  
sortie reliée à la seconde entrée du circuit  
comparateur de la carte, caractérisée en ce qu'elle  
20 comporte des moyens d'écriture (22) pouvant être  
reliés à ladite porte de commande d'écriture (13)  
de la carte pour mettre les éléments de mémoire de  
la zone transactionnelle (111) dans ledit état  
25 initial déterminé.

10- Machine d'effacement d'une carte suivant la reven-  
dication 7, comportant des moyens de lecture des  
zones accessibles de la mémoire de la carte quand  
celle-ci est connectée à la machine, un circuit  
30 cryptographique fonctionnant suivant ledit

35

algorithme et ayant son entrée pouvant être reliée  
à la deuxième zone de la mémoire de la carte et sa  
sortie reliée à la seconde entrée du circuit  
comparateur de la carte, caractérisée en ce qu'elle  
5 comporte un circuit opérateur numérique effectuant  
la différence entre la valeur fiduciaire lue dans  
le registre de la zone de mémoire transactionnelle  
et la somme des valeurs fiduciaires représentées  
par les éléments de mémoire dont l'état a été  
10 changé dans chaque groupe d'éléments, ledit circuit  
opérateur étant équipé d'un dispositif d'affichage  
de la différence ainsi calculée, et des moyens  
d'écriture prévus pour être reliés à ladite logique  
d'écriture de la carte.

15

20

25

30

35

FIG. 1

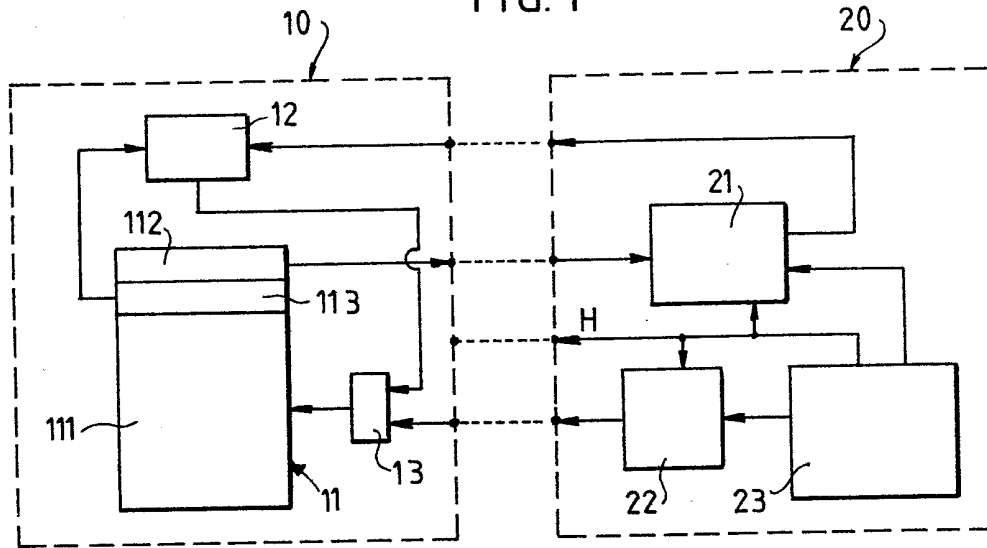


FIG. 2

