(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 803 961**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 00664**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.01.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.07.01 Bulletin 01/29.

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

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

(71) **Demandeur(s) :** *MORET GHISLAIN* — FR.

(72) **Inventeur(s) :** MORET GHISLAIN.

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

(74) **Mandataire(s) :** MORET DE ROCHEPRISE GHISLAIN.

(54) SYSTEME DE SECURISATION DES TRANSACTIONS LORS D'ACHATS PAR CORRESPONDANCE.

(57) Système de sécurisation des transactions lors d'achat par correspondance, notamment sur Internet, caractérisé par la délivrance d'un code unique et non réutilisable pour chaque transaction effectuée.

FR 2 803 961 - A1

2803961

La présente invention concerne un système de sécurisation des transactions lors d'achats par correspondance, notamment sur Internet ou minitel.

La vente de produits par correspondance, notamment sur Internet ou minitel, nécessite un système de paiement inviolable. Le principe actuellement le plus répandu est la communication par l'acheteur de ses cordonnées bancaires, via les coordonnées de sa carte de crédit. Ces informations sont transmises cryptées afin d'éviter la fraude. Cependant outre le fait que tout cryptage est réputé decryptable, et le besoin de prendre en considération la bonne foi du vendeur, les possibilités de fraudes par piratage informatique restent réelles tant que ce code est réutilisable anonymement.

Les alternatives existantes sont le paiement par chèque ou par mandat, bien moins pratiques pour le client.

La présente invention propose un système de paiement qui permet de résoudre les problèmes précités.

La transaction par correspondance, sécurisée selon l'invention, est caractérisée par l'utilisation d'un système électronique contenant dans une mémoire protégée une série de codes correspondants à une série de requêtes de la part de l'utilisateur. Cette table requêtes/codes est connue de la seule société émettrice de la carte, et tenue secrète.

La société émettrice faisant office d'établissement de banque ou étant associée à un établissement bancaire, est garante de la validité de la transaction. Le système électronique possède un microprocesseur ayant en charge la gestion interne des informations et les calculs nécessaires aux différents process, ainsi qu'une interface homme/machine sous la forme, par exemple, d'un clavier de 10 touches allant de 0 à 9 plus deux touches programmables, par exemple Validation et Annulation, et d'un écran de visualisation, voire d'un écran tactile faisant office de clavier.

La procédure de transaction telle que décrite par la présente invention se déroule ainsi : le dépositaire du système électronique précédemment décrit, nommé l'acheteur, se met en contact avec le vendeur. Pour le règlement de ses achats, le vendeur lui demande le numéro de série de son système électronique, lequel est unique

et noté sur le dit système, ainsi qu'un numéro d'achat et un numéro de certification. L'acheteur se fait alors reconnaître auprès de son système électronique par l'introduction d'un code de signature individuel, par exemple sous la forme d'un code à 4 chiffres, communément nommé code PIN (Personal Identification Number). Le système électronique possède un programme de surveillance vérifiant la validité de ce code, et bloquant son utilisation après trois essais infructueux successifs.

Après validation du code PIN, le système électronique délivre à l'acheteur un numéro d'achat issu d'un compteur interne. Ce numéro s'incrémente de un chaque fois que l'acheteur accède à un code de certification. Il correspond donc au nombre d'achat effectué par l'acheteur.

Dans une première version de la présente invention la table requête/code enregistrée dans la mémoire du système électronique fait correspondre à chacun des numéros d'achat un code défini aléatoirement lors de l'initialisation du système par la société émettrice.

Dans une seconde version de la présente invention la table requête/code enregistrée dans la mémoire est un algorithme de codage fournissant à la demande un code image du numéro d'achat.

Le spécialiste aura la possibilité de choisir telle ou telle version, en fonction de la vitesse de calcul et de l'espace mémoire disponible dans le système électronique, ainsi que de choisir le type d'algorithme parmi les algorithmes de cryptographie existants dans la littérature (US 4.405.829 ; FR 2.756.122 par exemple), ou pouvant être décrite dans le futur.

L'acheteur transmet ensuite au vendeur le numéro de série ainsi que les numéros d'achat et de certification délivrés par son système électronique. Le vendeur prend alors contact avec la société bancaire émettrice en lui fournissant ces informations, éventuellement à travers un réseau sécurisé. La société bancaire émettrice vérifie la validité de ces informations et enregistre l'utilisation de ce numéro d'achat. Elle fournit au vendeur un accord de transaction, ou effectue directement le paiement de la commande depuis le compte de l'acheteur, et éventuellement envoie par messagerie électronique un reçu à l'acheteur. Si ultérieurement elle reçoit un ordre d'achat comprenant un numéro d'achat ou un code secret déjà utilisé, elle refusera cet ordre et en avertira par messagerie électronique ou tout autre moyen le légitime détenteur de ce compte.

La durée entre l'instant où l'acheteur transmet l'information (numéro de série, numéro d'achat, code secret), et celui où la société émettrice enregistre cette utilisation devra être la plus courte possible. Ainsi si cette durée reste inférieure au temps nécessaire à son utilisation frauduleuse, on pourra parler de sécurité absolue du système.

Le format de la carte de crédit est si répandu et si adapté à la vie quotidienne, qu'il est souhaitable qu'une version de ce système électronique en ait le format. Cependant comme une interface utilisateur/système est nécessaire, on préconisera l'utilisation d'une carte ayant un clavier sensitif, ou de toute technologie de faible épaisseur, de 12 touches (0 à 9, valider, annuler), et un écran digital, une telle carte ayant par ailleurs déjà été décrite dans la littérature (FR 2 768 532). Le présent système électronique ne nécessitant en premier lieu pas de communication électronique extérieure, l'interface de communication par contact affleurant habituel sur les cartes à puces n'est pas nécessaire.

Cette interface pourra cependant apparaître dans le cas d'une carte hybride supportant d'autres fonctions que celle exposée précédemment. Il faudra alors prendre soin de conserver l'inviolabilité de la mémoire contenant la table requêtes/codes soit par une séparation physique des circuits à l'intérieur de la carte, soit par une séparation électronique de ces circuits.

Il pourra toutefois exister une zone de contacts affleurants, géographiquement bien définie sur le système électronique, comprenant deux pôles afin, soit d'alimenter le système en électricité pour son fonctionnement, soit d'alimenter le système en électricité pour recharger une batterie d'alimentation interne au système. L'alimentation électrique par cellule photoélectrique est également possible.

On peut également selon ce système, utiliser un support interface, tel qu'un téléphone portable par exemple ou un agenda électronique personnel, au sein duquel a été placé l'ensemble microprocesseur/table de données, en prenant soin de conserver la stricte impossibilité de lecture des données de la table par un quelconque accès externe. On peut, dans ce cas, rendre possible l'envoi à un correspondant d'un triplet (numéro de série / numéro d'achat / code secret) en utilisant le réseau téléphonique sous forme d'un signal numérique.

-REVENDICATIONS-

1- Dispositif de sécurisation des transactions de vente par correspondance délivrant un code secret unique et non réutilisable pour chaque transaction.

2- Dispositif de sécurisation des transactions de vente par correspondance caractérisé en ce qu'il comporte un système électronique individuel fournissant un code secret unique et non réutilisable permettant de certifier l'identité de l'acheteur.

3- Dispositif selon la revendication 2 caractérisé en ce que le système électronique comporte un clavier de 10 touches numérotées de 0 à 9, et deux touches permettant les fonctions validation et annulation.

4- Dispositif selon l'une quelconque des revendications 2 et 3 caractérisé en ce que le système électronique comporte un écran de visualisation.

5- Dispositif selon l'une quelconque des revendications 2 et 3 caractérisé en ce que le système électronique comporte un écran tactile.

6- Dispositif selon l'une quelconque des revendications 2 à 5 caractérisé en ce que l'utilisation du système électronique est contrôlée par l'entrée d'un code personnel.

7- Dispositif selon la revendication 6 caractérisé en ce que l'entrée à la suite de 3 codes différents du code personnel entraîne le blocage définitif d'accès aux codes secrets de sécurisation.

8- Dispositif selon la revendication 6 caractérisé en ce que l'entrée à la suite de 3 codes différents du code personnel entraîne le blocage d'accès aux codes secrets de sécurisation.

9- Dispositif selon l'une quelconque des revendications 2 à 8 caractérisé en ce que le système électronique a le format d'une carte de crédit.

10- Dispositif selon l'une quelconque des revendications 2 à 8 caractérisé en ce que le système électronique est un téléphone portable, ou un agenda électronique.

11- Dispositif selon l'une quelconque des revendications 2 à 10 caractérisé en ce que le système électronique possède un compteur incrémental s'incrémentant d'une unité a chaque fois que le système fournis un code de certification.

12- Dispositif selon la revendication 11 caractérisé en ce que le système électronique comporte une mémoire renfermant une table de correspondance entre les N incréments du compteur et N codes définis aléatoirement. Cette mémoire n'est accessible que par le circuit interne du système électronique, et sa table est connue et tenue secrète par la société émettrice déclarée garante des transactions à sécuriser. Les N codes sont les codes secrets de sécurisation.

13- Dispositif selon la revendication 11 caractérisé en ce que le système électronique comporte une mémoire renfermant un algorithme de transformation des N incréments du compteur. Cette mémoire n'est accessible que par le circuit interne du système électronique, et son algorithme est connu et tenu secret par la société émettrice déclarée garante des transactions à sécuriser. Les codes produits par la transformation des incréments du compteur grâce à l'utilisation de cet algorithme sont les codes secrets de sécurisation.

14- Procédé de transaction caractérisé par la délivrance par l'acheteur au vendeur d'un code secret renouvelé a chacune de ses transactions et non réutilisable, permettant à un tiers, par exemple une banque, de garantir l'identité de l'acheteur.

15- Procédé de transaction selon la revendication 14 caractérisé en ce que l'acheteur possède en son nom un dispositif de certificat de son identité tel que décris dans l'une quelconque des revendications 1 à 11, délivrant un code secret connu par la société émettrice, garante de la transaction, et que ce tiers, après corrélation entre le code secret et les éléments nécessaires à la reconnaissance de l'identité de l'acheteur accorde son aval à l'aboutissement de la transaction.

16- Procédé de transaction selon la revendication 14 caractérisé en ce que l'acheteur possède en son nom un dispositif selon l'une quelconque des revendications 12 ou 13, et que la manière dont le dispositif transforme la valeur du compteur incrémental en un code secret est connue et tenue secrète par la société émettrice, garante de la transaction, et que ce tiers, après corrélation entre le code secret, le numéro de série du dispositif, et le numéro d'achat ou la valeur du compteur incrémental, accorde son aval à l'aboutissement de la transaction.

17- Procédé de transaction selon l'une quelconque des revendications 15 ou 16 caractérisé en ce que le garant ayant mémorisé chaque combinaison reçue (numéro d'achat, numéro de série), vérifie avant de donner son aval que celle-ci n'a pas été précédemment utilisée, et émet un interdit sur la transaction dans le cas contraire.

18- Procédé de transaction selon la revendication 17 caractérisé en ce que chaque accord de transaction est notifié au légitime émetteur du code secret.

19- Procédé de transaction selon l'une quelconque des revendications 17 ou 18 caractérisé en ce que chaque refus de transaction est notifié au légitime émetteur du code secret.

20- Procédé de transaction selon l'une quelconque des revendications 15 à 19 caractérisé en ce que le temps écoulé entre l'émission du code secret de sécurisation et l'introduction de ce code dans la corrélation est suffisamment court pour interdire la possibilité d'une utilisation frauduleuse de ce code secret.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

2803961

N° d'enregistrement national

FA 587344
FR 0000664

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 5 606 614 A (BRADY PATRICK S ET AL) 25 février 1997 (1997-02-25) * abrégé; revendications; figures * ---	1-3,6,9, 11-18	H04L9/32 G06K19/07
A	US 5 317 636 A (VIZCAINO GERARDO) 31 mai 1994 (1994-05-31) * colonne 2, ligne 31 - colonne 8, ligne 6; figures 2,3 * ---	1-3,6,9, 11-18	
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 mars 1999 (1999-03-16) * abrégé; figures 1,4 * * colonne 5, ligne 24 - colonne 7, ligne 17 * ---	1,2,4,6, 9-18	
A	US 4 725 719 A (ONCKEN JOHN E ET AL) 16 février 1988 (1988-02-16) * le document en entier * ---	1,2,6,9, 14,15	
A	FR 2 471 000 A (DASSAULT ELECTRONIQUE) 12 juin 1981 (1981-06-12) * page 2, ligne 16 - page 3, ligne 8 * * page 8, ligne 15 - page 9, ligne 3 * ---	2,3,6-9	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G07F G06F
A	EP 0 010 496 A (CHATEAU MICHEL) 30 avril 1980 (1980-04-30) * abrégé; figure 2 * ---	1,14	
A	US 4 630 201 A (WHITE PETER) 16 décembre 1986 (1986-12-16) * le document en entier * ---	1,14	
A	US 5 802 497 A (MANASSE MARK S) 1 septembre 1998 (1998-09-01) * abrégé; revendications 1-11; figures 3,4 * --- -/--	1,14	

Date d'achèvement de la recherche	Examinateur
30 octobre 2000	Guivol, O

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

3

EPO FORM 1503 12.99 (P04C14)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

2803961

FA 587344
FR 0000664

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	FR 2 640 549 A (MORILLON ALAIN) 22 juin 1990 (1990-06-22) -----		

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

Date d'achèvement de la recherche	Examinateur
30 octobre 2000	Guivol, O

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

3

EPO FORM 1503 12.99 (P04C14)