(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 792 088**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 04395**

(51) Int Cl[7] : **G 06 F 17/60,** G 06 K 19/07, G 06 F 12/14, H 04 L 9/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 08.04.99.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 13.10.00 Bulletin 00/41.

(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) :** *FONTANIVE JEAN CLAUDE* — FR.

(72) **Inventeur(s) :** FONTANIVE JEAN CLAUDE.

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

(74) **Mandataire(s) :** NONY.

(54) PROCEDE DE PAIEMENT SECURISE ET DISPOSITIF POUR LA MISE EN OEUVRE D'UN TEL PROCEDE.

(57) Procédé de paiement sécurisé comportant les étapes consistant à:

a) fournir une carte à puce (1) à chaque utilisateur (U) d'une pluralité de groupes (G_q) d'utilisateurs, ($U_{s,q}$)

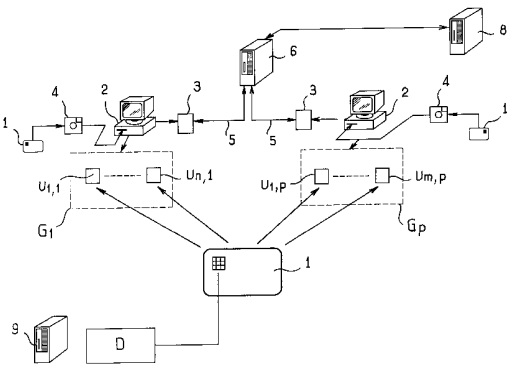
b) fournir à chaque groupe (G_q) d'utilisateurs au moins un micro-ordinateur (2), q

c) mémoriser dans la carte à puce (1) de chaque utilisateur des données (D) connues du serveur (6), permettant à ce dernier d'identifier l'utilisateur et le groupe d'utilisateurs auquel appartient celui-ci,

d) après connexion d'un utilisateur audit serveur, vérifier l'appartenance de cet utilisateur à l'un desdits groupes d'utilisateurs,

e) autoriser, dans l'affirmative, l'accès de l'utilisateur à des offres de produits et services prédéterminées.

f) en cas d'achat, vérifier le code confidentiel de l'utilisateur avant de valider le paiement.



FR 2 792 088 - A1

La présente invention concerne un procédé de paiement sécurisé et un dispositif pour la mise en œuvre d'un tel procédé.

De nombreux produits et services sont aujourd'hui offerts à la vente sur Internet.

Le plus souvent, le paiement s'effectue en donnant un numéro de carte de crédit.

Des procédés de paiement sécurisé ont été proposés, faisant intervenir l'encryptage de données.

Toutefois, ces procédés de paiement sécurisé connus n'offrent pas entière satisfaction, et l'on constate encore une certaine appréhension des utilisateurs à effectuer leurs achats sur Internet, par crainte de piratage des informations bancaires.

La présente invention vise à proposer un nouveau procédé de paiement sécurisé, destiné au commerce électronique, qui soit sûr et relativement peu coûteux à mettre en œuvre.

Le procédé de paiement sécurisé selon l'invention est caractérisé par le fait qu'il comporte les étapes consistant à :

a) fournir une carte à puce à chaque utilisateur d'une pluralité de groupes d'utilisateurs,

b) fournir si nécessaire à chaque groupe d'utilisateurs au moins un micro-ordinateur, équipé d'une part d'un modem permettant la connexion à un serveur via un réseau de télécommunications et d'autre part d'une interface permettant de lire des cartes à puce,

c) mémoriser dans la carte à puce de chaque utilisateur des données connues du serveur, permettant à ce dernier d'identifier l'utilisateur et le groupe d'utilisateurs auquel appartient celui-ci et de valider un code confidentiel spécifique à l'utilisateur,

d) après connexion d'un utilisateur audit serveur au moyen d'un micro-ordinateur équipé d'un modem permettant la connexion audit serveur via ledit réseau de télécommunications et d'une interface permettant de lire la carte à puce attribuée à cet utilisateur, vérifier l'appartenance de cet utilisateur à l'un desdits groupes d'utilisateurs par lecture de données mémorisées dans ladite carte à puce et comparaison avec des données connues du serveur,

e) autoriser, dans l'affirmative, l'accès de l'utilisateur à des offres de produits et services prédéterminées,

f) en cas d'achat, vérifier le code confidentiel de l'utilisateur avant de valider le paiement.

La sécurité du paiement est garantie par l'invention d'une manière efficace, grâce au fait que des vérifications multiples à la fois matérielles et informatiques sont effectuées à plusieurs niveaux, rendant de ce fait difficile le piratage informatique.

Tout d'abord, chaque transaction est subordonnée à la détention matérielle par l'utilisateur, au moment de l'achat, de la carte à puce dans laquelle sont mémorisées des informations connues du serveur.

Ensuite, les cartes à puces ne sont délivrées qu'à des utilisateurs choisis parmi des groupes d'utilisateurs prédéterminés, ce qui contribue non seulement à la sécurité de l'utilisateur mais aussi à celle des fournisseurs de produits ou services mis à la disposition des utilisateurs par le serveur, puisque le groupe d'utilisateurs auquel appartient l'utilisateur peut être choisi en fonction de critères prédéterminés, notamment de solvabilité.

Enfin, toute transaction ne peut s'effectuer qu'après la lecture de données mémorisées dans la carte à puce pour identifier l'utilisateur et le groupe d'utilisateurs auquel il appartient et vérification d'un code confidentiel spécifique à l'utilisateur.

Dans une mise en œuvre préférée de l'invention, l'utilisateur ne fournit qu'une seule fois au serveur les coordonnées bancaires du compte qu'il souhaite voir débiter lors des transactions, le serveur conservant en mémoire ces coordonnées bancaires.

Ainsi, l'utilisateur n'a plus à donner ses coordonnées bancaires lors des transactions suivantes, ce qui diminue les risques d'interception par un pirate informatique desdites coordonnées bancaires, à la différence des procédés de paiement sécurisés connus, lesquels exigent qu'à chaque transaction l'utilisateur fournisse ses coordonnées bancaires, qui bien qu'encryptées restent toujours susceptibles d'être interceptées.

Toujours dans une mise en œuvre préférée de l'invention, l'interface précitée comporte un support ayant la forme générale extérieure d'une disquette, apte à être introduite dans un lecteur de disquettes du micro-ordinateur.

De cette façon, la carte à puce peut être lue par pratiquement n'importe quel micro-ordinateur, sans nécessiter d'effectuer de nouveaux branchements sur les ports série ou parallèle, souvent déjà utilisés pour des périphériques.

L'invention a encore pour objet un dispositif pour la mise en œuvre du procédé défini plus haut, ce dispositif étant caractérisé par le fait qu'il comporte :

- un ensemble de cartes à puce pour chacun des utilisateurs d'une pluralité de groupes d'utilisateurs,
- un serveur,
- au moins un micro-ordinateur pour chaque groupe d'utilisateurs, chaque micro-ordinateur étant équipé d'un modem permettant la connexion audit serveur via un réseau de télécommunications et d'une interface permettant de lire des cartes à puce,
- des moyens pour mémoriser dans chaque carte à puce des données connues du serveur permettant à ce dernier d'identifier l'utilisateur et le groupe d'utilisateurs auquel celui-ci appartient et de valider un code confidentiel spécifique à l'utilisateur.

L'invention a encore pour objet un ensemble de cartes à puce destinées à un groupe d'utilisateurs, pour la mise en œuvre du procédé tel que défini plus haut.

L'invention sera mieux comprise à la lecture de la description détaillée qui va suivre, d'un exemple de mise en œuvre non limitatif et à l'examen de la figure unique du dessin annexé.

Dans l'exemple illustré, on adresse à chaque utilisateur d'une pluralité de groupes d'utilisateurs une carte à puce 1 dont la structure est connue en elle-même, chaque carte à puce 1 comportant une mémoire non volatile capable de mémoriser des informations.

On suppose dans l'exemple décrit qu'il y a p groupes d'utilisateurs G_1, ...,G_P, chaque groupe G_q ($1 \leq q \leq p$)comportant un nombre r(q) donné d'utilisateurs $U_{s,q}$ ($1 \leq s \leq r(q)$).

Conformément à l'invention, chaque groupe d'utilisateurs G_q dispose d'un micro-ordinateur 2 équipé d'un modem 3 et d'un lecteur de disquettes 3.5"

Chaque groupe d'utilisateur G_q est constitué par exemple par les salariés d'une même entreprise, le micro-ordinateur 2 étant alors avantageusement mis à la disposition du comité d'entreprise.

Le modem 3 permet la connexion à un serveur 6, via un réseau de télécommunications 5.

Cette connexion s'effectue dans l'exemple décrit par le réseau Internet.

Chaque micro-ordinateur 2 comporte une interface 4 permettant la lecture de cartes à puce, chaque interface 4 ayant dans l'exemple de réalisation décrit la forme générale extérieure d'une disquette 3.5".

L'interface 4 est destinée à être introduite dans le lecteur de disquettes 3.5" du micro-ordinateur 2.

L'interface comporte des moyens permettant l'échange de données d'une part avec les circuits électroniques de la carte à puce 1 et d'autre part avec la tête magnétique du lecteur de disquettes 3.5" du micro-ordinateur 2.

Le serveur 6 est interconnecté au serveur 8 d'une banque, pour débiter les comptes bancaires des utilisateurs lors des transactions.

Préalablement à l'envoi des cartes à puce 1 aux utilisateurs, des données D sont mémorisées dans chaque carte à puce 1, par des moyens d'écriture 9 connus en eux-mêmes.

Ces données D comportent un code d'identification spécifique à chaque utilisateur et des informations permettant au serveur 6 d'identifier chaque utilisateur connecté ainsi que le groupe d'utilisateurs auquel celui-ci appartient, comme cela va être précisé plus loin.

Lorsque l'utilisateur appartenant à un groupe d'utilisateur G_q désire effectuer un achat, il introduit sa carte à puce 1 dans l'interface 4, laquelle est ensuite mise en place dans le lecteur de disquettes 3.5" du micro-ordinateur 2.

Cet utilisateur se connecte alors au serveur 6, via le réseau de télécommunications 5.

Lors de la connexion, le serveur 6 vérifie, par lecture d'informations contenues dans la carte à puce 1 et comparaison avec des données connues du serveur 6, l'appartenance de l'utilisateur à l'un des groupes d'utilisateurs G_1, ...,G_P et, dans l'affirmative, autorise l'utilisateur à accéder à des offres de produits et services prédéterminées.

Au moment de passer un achat, l'utilisateur compose son code confidentiel sur le clavier du micro-ordinateur 2, après que le serveur 6 le lui ai demandé.

Dans l'exemple décrit, le serveur 6 demande en outre à l'utilisateur lors de la première transaction, d'indiquer ses coordonnées bancaires.

Ces coordonnées bancaires sont mémorisées dans le serveur 6 pour les transactions suivantes.

Ainsi, au cours de ces dernières, le serveur 6 adresse directement au serveur bancaire 8 l'ordre de débiter le compte de l'utilisateur connecté d'un montant donné, sans que cet utilisateur ait à nouveau à faire transiter sur Internet ses coordonnées bancaires.

Bien entendu, l'invention n'est pas limitée à l'exemple de réalisation décrit.

On peut notamment, sans sortir du cadre de la présente invention, se servir d'un autre type d'interface permettant de lire des cartes à puce, et utiliser par exemple des micro-ordinateurs comportant des lecteurs de cartes à puce intégrés.

REVENDICATIONS

1. Procédé de paiement sécurisé, caractérisé par le fait qu'il comporte les étapes consistant à :

a) fournir une carte à puce (1) à chaque utilisateur ($U_{s,q}$) d'une pluralité de groupes (G_q) d'utilisateurs,

b) fournir si nécessaire à chaque groupe (G_q) d'utilisateurs au moins un micro-ordinateur (2), équipé d'une part d'un modem (3) permettant la connexion à un serveur via un réseau de télécommunications (5) et d'autre part d'une interface (4) permettant de lire des cartes à puce,

c) mémoriser dans la carte à puce(1) de chaque utilisateur des données (D) connues du serveur (6), permettant à ce dernier d'identifier l'utilisateur et le groupe d'utilisateurs auquel appartient celui-ci et de valider un code confidentiel spécifique à l'utilisateur,

d) après connexion d'un utilisateur audit serveur au moyen d'un micro-ordinateur équipé d'un modem permettant la connexion audit serveur via ledit réseau de télécommunications et d'une interface (4) permettant de lire la carte à puce attribuée à cet utilisateur, vérifier l'appartenance de cet utilisateur à l'un desdits groupes d'utilisateurs par lecture de données (D) mémorisées dans ladite carte à puce et comparaison avec des données connues du serveur (6),

e) autoriser, dans l'affirmative, l'accès de l'utilisateur à des offres de produits et services prédéterminées,

f) en cas d'achat, vérifier le code confidentiel de l'utilisateur avant de valider le paiement.

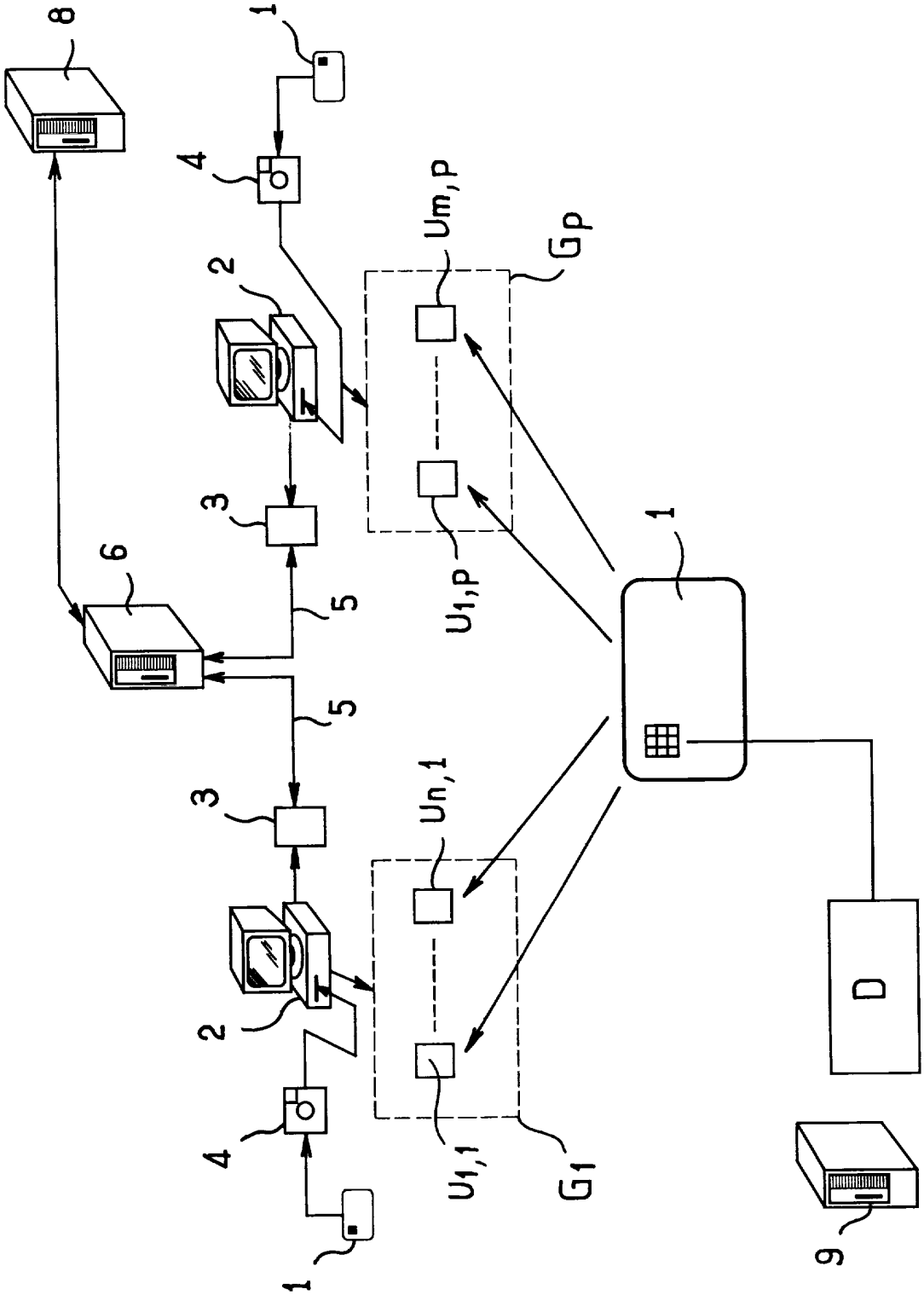
2. Procédé selon la revendication 1, caractérisé par le fait que l'utilisateur ($U_{s,q}$) ne fournit qu'une seule fois au serveur (6) les coordonnées bancaires du compte qu'il souhaite voir débiter lors de toutes les transactions, le serveur (6) conservant en mémoire ces coordonnées bancaires.

3. Procédé selon l'une quelconque des revendications précédentes, caractérisé par le fait que l'interface (4) comporte un support ayant la forme générale extérieure d'une disquette 3.5", apte à être introduite dans le lecteur de disquettes du micro-ordinateur (2).

4. Dispositif pour la mise en œuvre du procédé selon l'une quelconque des revendications précédentes, caractérisé par le fait qu'il comporte :

- un ensemble de cartes à puce (1) pour chacun des utilisateurs ($U_{s,q}$) d'une pluralité de groupes (G_q) d'utilisateurs,
- un serveur (6),
- au moins un micro-ordinateur (2) pour chaque groupe (G_q) d'utilisateurs, chaque micro-ordinateur (2) étant équipé d'un modem (3) permettant la connexion à ce serveur (6) via un réseau de télécommunications (5) et d'une interface (4) permettant de lire des cartes à puce,
- des moyens (9) pour mémoriser dans chaque carte à puce des données connues du serveur (6) permettant d'identifier l'utilisateur ($U_{s,\ q}$) et le groupe d'utilisateurs (G_q) auquel celui-ci appartient et de valider un code confidentiel spécifique à l'utilisateur.

5. Ensemble de cartes à puce (1) destinées à un groupe (G_q) d'utilisateurs pour la mise en œuvre du procédé tel que défini dans l'une quelconque des revendications 1 à 3.


8
1
4
2
3
6
5
5
3
2
4
1
Um,p
Gp
U1,p
1
Un,1
U1,1
G1
D
9

REPUBLIQUE FRANÇAISE

2792088

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

N° d'enregistrement national

FA 571501
FR 9904395

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	WO 95 12856 A (SMART PAYMENT SYSTEMS LTD ;BLEARS RICHARD (GB)) 11 mai 1995 (1995-05-11) * page 3, alinéa 1 - page 7, alinéa 4 * * page 9, ligne 2 - page 12, ligne 1 *	1-5
Y	WO 98 11497 A (HYPERCOM INC ;WALLNER GEORGE (US)) 19 mars 1998 (1998-03-19) * page 5, ligne 2 - page 6, ligne 2 * * figure 1 *	1-5
A	US 5 770 843 A (HOEVEL LEE W ET AL) 23 juin 1998 (1998-06-23) * abrégé * * colonne 2, ligne 38 - colonne 4, ligne 67 * * revendication 1; figure 5 *	1
A	US 5 223 894 A (ITO MASAZUMI) 29 juin 1993 (1993-06-29)	
A	DE 197 16 068 A (GIESECKE & DEVRIENT GMBH) 22 octobre 1998 (1998-10-22)	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07F

Date d'achèvement de la recherche: 14 décembre 1999

Examinateur: Bocage, S

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
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

EPO FORM 1503 03.82 (P04C13)