(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 914 763**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **07 02551**

(51) Int Cl[8] : ***G 06 Q 20/00*** *(2006.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.04.07.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 10.10.08 Bulletin 08/41.

(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) :** *GROUPEMENT DES CARTES BANCAIRES* — FR.

(72) **Inventeur(s) :** MEGGLE CLAUDE et CHASSIGNEUX PIERRE.

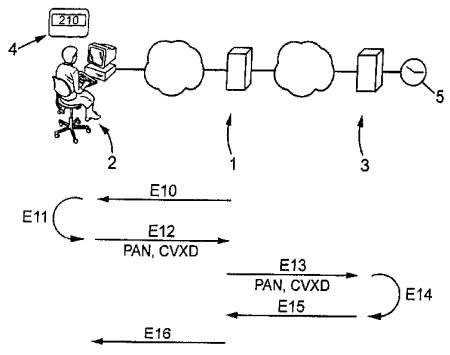
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) CRYPTOGRAMME DYNAMIQUE.

(57) Un procédé de validation d'une transaction à distance utilisant une carte bancaire gérée par un organisme financier, entre un débiteur (2) titulaire de ladite carte et un créancier (1), comporte .

- la réception (E13) d'une requête de validation en provenance du créancier par un serveur (3) de l'organisme financier, comportant au moins le numéro de carte (PAN) et un champ de données (CVXD) associé à la carte et variant avec chaque transaction effectuée par le débiteur avec sa carte; et
- la vérification (E14) par l'organisme financier que le champ de données correspond effectivement à la carte; et
- l'émission (E15) par le serveur de l'organisme financier à destination du créancier d'une autorisation de transaction si la vérification est positive.



FR 2 914 763 - A1

CRYPTOGRAMME DYNAMIQUE

La présente invention concerne un procédé et un serveur de validation d'une transaction financière exécutée à distance à l'aide d'une carte bancaire. Elle concerne également un produit programme d'ordinateur pour mettre en œuvre le procédé de validation.

Lors de vente à distance via le réseau internet ou par téléphone, le moyen de paiement le plus utilisé est la carte bancaire. A cet effet, figure 1, le protocole le plus couramment utilisé consiste pour le commerçant 1, c'est-à-dire le créancier de la transaction, à demander à son client 2, le débiteur de la transaction, le numéro et la date de fin de validité d'une carte de paiement, étapes E1 - E2 puis à transmettre, étape E3, ces informations avec d'autres données liées à la transaction telles que le montant de celle-ci ou l'identifiant du commerçant à la banque 3, gestionnaire de la carte.

La banque 3 vérifie, étape E4, la cohérence des données transmises, le montant de la transaction par rapport à un plafond de dépenses autorisées, etc. et envoie, étape E5, un message de validation au commerçant, message comportant un numéro de validation. Le commerçant transmet, étape E6, au client une copie du message de validation et enclenche, étape E7, le processus de livraison du produit ou service commandé.

Or ce protocole est relativement aisé à frauder dans la mesure où les numéros de carte sont facilement accessibles et les dates de validité ne varient qu'entre 24 ou 36 valeurs possibles (les mois des deux ou trois prochaines années).

Ainsi, par exemple, il existe des logiciels dans

lesquels, après qu'un numéro de carte valide a été saisi, ceux-ci exécutent des transactions en essayant automatiquement différentes dates de fin de validité.

Pour renforcer la sécurité des transactions et s'assurer que, au minimum le client est réellement en possession de la carte, il lui est demandé de saisir en plus un numéro de 3 ou 4 chiffres imprimé le plus souvent au dos de la carte. Le numéro n'est pas embossé et son lien avec la carte n'est connu que de la banque émettrice de la carte.

Ce numéro, appelé souvent dans la littérature « cryptogramme visuel » est également connu sous les références CVX2 pour le Groupement d'Intérêt Economique Cartes Bancaires (France), CVV2 pour VISA (USA) ou CVC2 pour Mastercard (USA).

Le protocole de transmission entre les créanciers et les banques est actuellement le plus souvent basé sur SSL (*Secure Socket Layer*, Couche Sécurisée de Sockets) ou TLS (*Transport Layer Security*, Sécurité de la Couche Transport).

Le protocole prévoit, de façon standardisé, le transport du cryptogramme visuel dans la requête de validation d'une transaction.

Cependant, bien que par convention les commerçants s'engagent à ne pas stocker le cryptogramme visuel, l'homme du métier peut aisément imaginer différentes attaques relativement faciles à mettre en œuvre pour récupérer, avec le numéro de la carte, la valeur du cryptogramme visuel.

Aussi serait-il souhaitable de disposer d'un procédé de validation qui renforce la sécurité des transactions à distance par carte sans modifier les protocoles de liaison entre les commerçants et les organismes financiers.

Pour résoudre ce problème, selon un aspect de

l'invention, un procédé de validation d'une transaction à distance utilisant une carte bancaire, entre un débiteur titulaire de ladite carte et un créancier, ladite carte étant associée à un compte géré par un organisme financier, et étant identifiée par au moins un numéro de carte, comporte :

- la réception d'une requête de validation en provenance du créancier par un serveur de l'organisme financier, ladite requête étant transmise par un réseau de données, ladite requête comportant au moins le numéro de carte et un champ de données associé à la carte ; et
- la vérification par l'organisme financier que le champ de données correspond effectivement à la carte, et
- l'émission par le serveur de l'organisme financier à destination du créancier par l'intermédiaire du réseau de données, d'une autorisation de transaction si la vérification est positive.

Le procédé est tel que le champ de données varie avec chaque transaction effectuée par le débiteur avec sa carte.

Ainsi le champ de données, ou cryptogramme visuel, ne permet pas, avantageusement, à un tiers de rejouer la transaction avec les mêmes paramètres.

Dans des modes de réalisation particuliers :

- la vérification du champ de données consiste à vérifier la valeur dudit champ dans une liste finie de valeurs non utilisées lors d'une transaction précédente ; ainsi, cela permet avantageusement de gérer les problèmes de synchronisation éventuelle entre le titulaire de la carte et l'organisme financier ;
- le débiteur possède un dispositif indépendant du réseau des données adapté pour fournir au débiteur le

champ de données à utiliser pour la transaction ; ce qui permet avantageusement de se protéger d'une attaque menée en écoutant le réseau de données ;

- ledit dispositif comporte une horloge synchronisée avec une horloge reliée au serveur de l'organisme financier, ledit champ de données étant calculés à partir de la date et de l'heure à laquelle le débiteur a demandé un champ de données audit dispositif ;
- le serveur de l'organisme financier n'accepte la transaction que si le champ de données correspond à une fenêtre de temps prédéterminée par rapport à la réception de la requête de validation ;
- le dispositif comporte un numéro de série utilisé pour diversifier le champ de données, ledit numéro de série étant associé au compte du débiteur par le serveur de l'organisme financier ;
- la carte est une carte à microprocesseur et le dispositif comporte des moyens d'interface avec ledit microprocesseur tel que la génération du champ de données est effectué par le microprocesseur après que le débiteur a installé sa carte dans ledit dispositif et demandé la génération d'un champ de données ;
- le dispositif est un terminal de télécommunication adapté pour recevoir des messages alphanumériques et en ce que le débiteur demande un champ de données par envoi d'un message au serveur et que celui-ci lui envoie ledit champ de données par un message alphanumérique reçu sur le terminal de télécommunication ;
- le numéro d'appel dudit terminal de télécommunication est préalablement enregistré dans les moyens de stockage du serveur financier de telle sorte que le champ de données n'est envoyé sur le terminal de télécommunication que si la demande de champ de

données est générée à partir dudit terminal de télécommunication.

Selon un second aspect de l'invention, un serveur de validation d'une transaction à distance utilisant une carte bancaire entre un débiteur titulaire de ladite carte et un créancier, ladite carte étant identifiée par au moins un numéro de carte, comporte :

- des moyens de connexion à un réseau de données adapté pour transmettre des messages de données entre le créancier et le serveur,
- des moyens de réception d'une requête de validation de la transaction en provenance du créancier par l'intermédiaire du réseau de données, ladite requête comportant au moins le numéro de la carte et un champ de données associé à la carte,
- des moyens de vérification que le champ de données est correctement associé à la carte,
- des moyens d'émission d'un message de validation de la transaction à destination du créancier par l'intermédiaire du réseau de données, lesdits moyens d'émission n'étant activés que si la vérification du champ de données est positive.

Le serveur de validation est tel que le champ de données varie avec chaque transaction effectuée par le débiteur avec sa carte.

Selon un troisième aspect de l'invention, un produit programme d'ordinateur comprend des instructions de code de programme pour l'exécution des étapes du procédé précédent lorsque ledit programme est exécuté sur un ordinateur.

L'invention sera mieux comprise à la lecture de la description qui suit, donnée uniquement à titre d'exemple, et faite en référence aux dessins en annexe dans lesquels :

- la figure 1 est une vue schématique d'un système de transaction à distance utilisant une carte bancaire selon l'art antérieur ;
- la figure 2 est une vue schématique d'un système de transaction à distance et du procédé de validation utilisant une carte bancaire selon un premier mode de réalisation de l'invention ;
- la figure 3 est une vue schématique d'un deuxième mode de réalisation d'un procédé selon l'invention ;
- la figure 4 est une vue schématique d'un troisième mode de réalisation d'un procédé selon l'invention ; et
- la figure 5 est une vue schématique d'un serveur de validation selon un mode de réalisation de l'invention.

Dans les différents dessins, un élément identique ou similaire porte une référence identique.

En référence à la figure 2, le client a à sa disposition un petit dispositif 4 portable dit « *token* » comportant une horloge, un numéro de série ou diversificateur et un petit écran.

L'horloge du « *token* » est adaptée pour rester synchronisée en permanence, dans une plage d'erreur prédéterminée, avec une horloge 5 reliée au serveur de la banque.

Lors de l'initialisation du « *token* », par exemple lors de la remise de celui-ci par les services de la banque au client, le diversificateur est stocké dans le serveur 3 de la banque en association avec le numéro de la carte.

Au cours d'une transaction, le commerçant 2 demande classiquement au client le numéro de carte, la date de fin de validité et le cryptogramme visuel.

Le client consulte, étape E11, alors son

« *token* » et indique, étape E12, comme cryptogramme visuel, le nombre CVXD apparaissant sur l'écran, ainsi que son numéro de carte PAN.

Ce nombre CVXD est calculé par le « *token* » selon un algorithme Alg1 connu et défini par la banque émettrice, l'algorithme prenant en paramètres d'entrée la date et l'heure de l'horloge au moment de la demande de CVXD et le diversificateur.

Le CVXD est envoyé, étape E13, par le commerçant à la banque selon le protocole habituel, la valeur CVXD prenant la place du champ CVX2.

A réception de la requête, le serveur extraie, étape E14, le diversificateur correspondant au numéro de carte PAN et exécute l'algorithme Alg1 en utilisant l'heure de réception de la requête et le diversificateur.

Si le nombre ainsi obtenu est égal au nombre CVXD envoyé, cela indique que le client est en possession du « *token* » et est donc bien le propriétaire de la carte. La transaction est alors validée, étapes E15 - E16, selon les règles habituelles du protocole.

Il est à noter que, de par le mode de fonctionnement, l'heure de demande d'un CVXD au « *token* » précède de quelques secondes ou minutes l'heure de réception de la requête de validation.

Afin de résoudre ce décalage, différentes méthodes sont utilisables et connues de l'homme du métier.

Par exemple, l'heure servant de base au calcul est arrondie à quelques minutes près, par exemple aux minutes multiples de 5.

Ainsi, de façon générale, l'heure de demande et l'heure de réception appartiennent au même intervalle. Si, par hasard, les deux heures se trouvent dans deux intervalles successifs, le serveur est programmé pour vérifier que, si le CVXD a été calculé avec l'heure de

l'intervalle précédent, la transaction également soit validée.

Dans un deuxième mode de réalisation, figure 3, le client reçoit un dispositif 6 appelé certificateur. Un certificateur est un dispositif se présentant sous la forme d'une calculette disposant d'une interface électrique avec la puce 7 d'une carte bancaire 8.

Lors d'une transaction pour obtenir, étape 21, un cryptogramme visuel, le client introduit sa carte 8 dans le certificateur 6, tape son code secret et le certificateur affiche un code CVXD que le client saisit dans le champ correspondant du formulaire du commerçant.

Comme lors du mode de réalisation précédent, le champ CVXD est transmis, étape E23, au serveur de la banque. Celui-ci est connecté à une boîte noire possédant les mêmes algorithmes de calcul que la puce de la carte. Le serveur fournit à la boîte noire le numéro de la carte et celui-ci calcule le cryptogramme visuel correspondant qui est comparé au cryptogramme visuel transmis.

Le calcul du cryptogramme visuel est avantageusement diversifié en utilisant le montant de la transaction, donnée qui est classiquement transmise par le commerçant dans la requête de validation.

Dans un troisième mode de réalisation, figure 4, le client est en possession d'un terminal 9 de télécommunication mobile tel qu'un téléphone GSM.

Lors de l'inscription au service, l'utilisateur indique à sa banque le numéro d'appel de son téléphone mobile.

Lors de la saisie des éléments de transaction, le client demande, étape E31, à sa banque un cryptogramme visuel CVXD.

Cette demande est indépendante des liaisons avec le commerçant. Par exemple, le client envoie un message court à un serveur de message court, ou bien il fait sa

demande auprès d'un serveur vocal.

En retour, la banque envoie, étape E32, le cryptogramme visuel CVXD à utiliser pour la transaction. Cet envoi se fait obligatoirement sur le téléphone référencé lors de l'inscription au service pour éviter une tentative d'obtention d'un cryptogramme visuel par une personne non habilitée.

Si le téléphone ne cache pas son numéro lors d'un appel, l'envoi se fait avantageusement dans l'appel de demande après vérification que celui-ci est bien initié par le téléphone enregistré. Ainsi, dans le cas d'un serveur vocal, celui-ci dicte au client, en réponse à sa demande, le cryptogramme visuel à saisir.

A la réception, étape E34, de la requête de validation envoyée par le commerçant, le serveur vérifie, étape E35, alors que le cryptogramme visuel transmis par la requête est le même que celui envoyé par téléphone.

Par rapport à un serveur classique de validation géré par un organisme financier, dans les modes de réalisation décrits, le serveur doit être adapté pour gérer les cryptogrammes visuels dynamiques.

Ainsi, dans un mode de réalisation, figure 5, le serveur de validation comporte des moyens 40 de connexion au réseau de données pour transmettre et recevoir des messages de données avec le créancier.

Il comporte également des moyens 42 de réception de la requête de validation de la transaction, requête provenant du créancier et comportant au moins le numéro de la carte et un champ de données associé à la carte.

Il comporte des moyens 44 de vérification de la validité du champ de données en relation avec le numéro de carte et des moyens 46 d'émission d'un message de validation à destination du créancier. Les moyens 46 d'émission ne sont activés que si le champ de données est validé.

On comprend que le procédé décrit dans ses divers modes de réalisation peut être mis en œuvre sous la forme d'un produit programme d'ordinateur exécuté sur un ordinateur.

Cet ordinateur peut être un ordinateur classique ou combiner un ordinateur classique avec des éléments spécifiques tels qu'une boite noire de calcul cryptographique, un serveur vocal ou un serveur de messages courts, une horloge, etc.

L'homme du métier sait, à partir des descriptions de ces modes de réalisation et des revendications, réaliser de nombreuses autres variantes de réalisation.

Par exemple, la banque peut fournir au client une liste de nombres CVXD à usage unique sous forme, par exemple, d'une feuille à gratter. A chaque transaction, le client gratte dans un ordre prédéfini une zone pour faire apparaître un numéro. Le serveur possède alors dans une zone de stockage la même liste associée au numéro de la carte pour effectuer les vérifications.

De même, selon les modes de réalisation, et les enjeux de protection, le procédé tolère que le cryptogramme visuel envoyé dans la requête de validation fasse partie d'une courte liste de cryptogrammes visuels valides tel qu'il a été décrit, par exemple, avec le premier mode de réalisation utilisant un « *token* ».

On a ainsi décrit un procédé et un serveur de validation de transaction qui permet d'augmenter significativement le degré de protection contre les fraudes en limitant les possibilités de rejeux sans modifier le protocole de gestion des transactions entre le client, le commerçant et la banque.

REVENDICATIONS

1. Procédé de validation d'une transaction à distance utilisant une carte bancaire, entre un débiteur titulaire de ladite carte et un créancier, ladite carte étant associée à un compte géré par un organisme financier, et étant identifiée par au moins un numéro de carte ledit procédé comportant :

- la réception (E13, E23, E34) d'une requête de validation en provenance du créancier par un serveur de l'organisme financier, ladite requête étant transmise par un réseau de données, ladite requête comportant au moins le numéro de carte (PAN) et un champ de données (CVXD) associé à la carte ; et
- la vérification (E14, E24, E35) par l'organisme financier que le champ de données correspond effectivement à la carte, et
- l'émission (E15, E25, E36) par le serveur de l'organisme financier à destination du créancier par l'intermédiaire du réseau de données, d'une autorisation de transaction si la vérification est positive;

caractérisé en ce que le champ de données varie avec chaque transaction effectuée par le débiteur avec sa carte.

2. Procédé selon la revendication 1, caractérisé en ce que la vérification du champ de données consiste à vérifier la valeur dudit champ dans une liste finie de valeurs non utilisées lors d'une transaction précédente.

3. Procédé selon les revendications 1 et 2, caractérisé en ce que le débiteur possède un dispositif indépendant du réseau des données adapté pour fournir au

débiteur le champ de données à utiliser pour la transaction.

4. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce que ledit dispositif comporte une horloge synchronisé avec une horloge reliée au serveur de l'organisme financier, ledit champ de données étant calculé à partir de la date et de l'heure à laquelle le débiteur a demandé un champ de données audit dispositif.

5. Procédé selon la revendication 4, caractérisé en ce que le serveur de l'organisme financier n'accepte la transaction que si le champ de données correspond à une fenêtre de temps prédéterminée par rapport à la réception de la requête de validation.

6. Procédé selon les revendications 4 et 5, caractérisé en ce que le dispositif comporte un numéro de série utilisé pour diversifier le champ de données, ledit numéro de série étant associé au compte du débiteur par le serveur de l'organisme financier.

7. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce que la carte est une carte à microprocesseur et le dispositif comporte des moyens d'interface avec ledit microprocesseur tel que la génération du champ de données est effectué par le microprocesseur après que le débiteur a installé sa carte dans ledit dispositif et demande la génération d'un champ de données.

8. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce que le dispositif est un terminal de télécommunication adapté pour recevoir des messages alphanumériques et en ce que le débiteur demande un champ de données par envoi d'un message au serveur et que celui-ci lui envoie ledit champ de données par un message alphanumérique reçu sur le terminal de télécommunication.

9. Procédé selon la revendication 8, caractérisé en ce que le numéro d'appel dudit terminal de

télécommunication est préalablement enregistré dans les moyens de stockage du serveur financier de telle sorte que le champ de données n'est envoyé sur le terminal de télécommunication que si la demande d'un champ de données est générée à partir dudit terminal de télécommunication.

10. Serveur de validation d'une transaction à distance utilisant une carte bancaire entre un débiteur titulaire de ladite carte et un créancier, ladite carte étant identifiée par au moins un numéro de carte, comportant :

- des moyens (40) de connexion à un réseau de données adapté pour transmettre des messages de données entre le créancier et le serveur,
- des moyens (42) de réception d'une requête de validation de la transaction en provenance du créancier par l'intermédiaire du réseau de données, ladite requête comportant au moins le numéro de la carte et un champ de données associé à la carte,
- des moyens (44) de vérification que le champ de données est correctement associé à la carte,
- des moyens (46) d'émission d'un message de validation de la transaction à destination du créancier par l'intermédiaire du réseau de données, lesdits moyens d'émission n'étant activés que si la vérification du champ de données est positive,

caractérisé en ce que

le champ de données varie avec chaque transaction effectuée par le débiteur avec sa carte.

11. Produit programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une quelconque des revendications 1 à 9 lorsque ledit programme est exécuté sur un ordinateur.

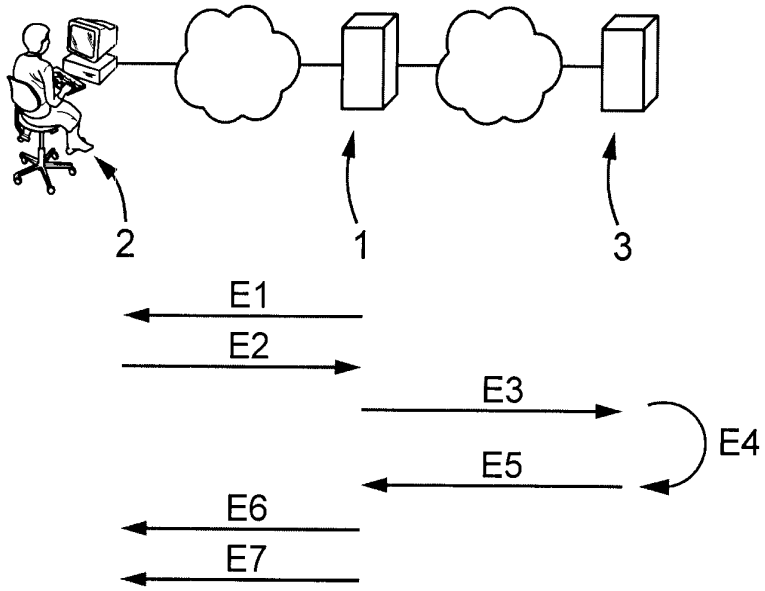


FIG. 1
(ART ANTÉRIEUR)

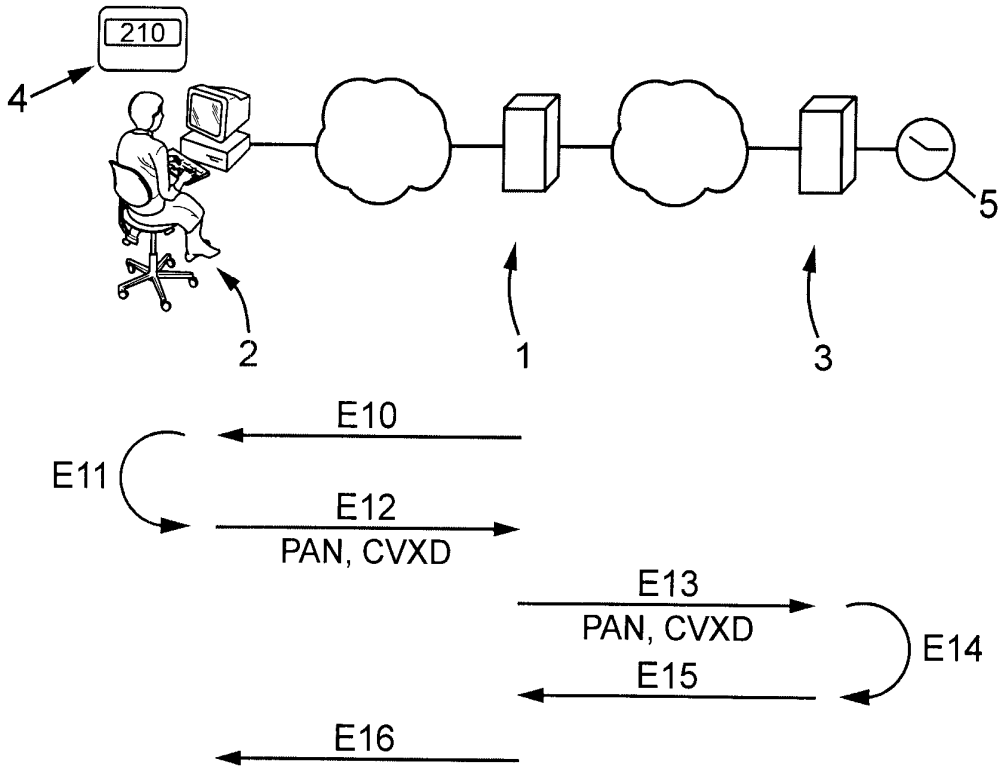


FIG. 2

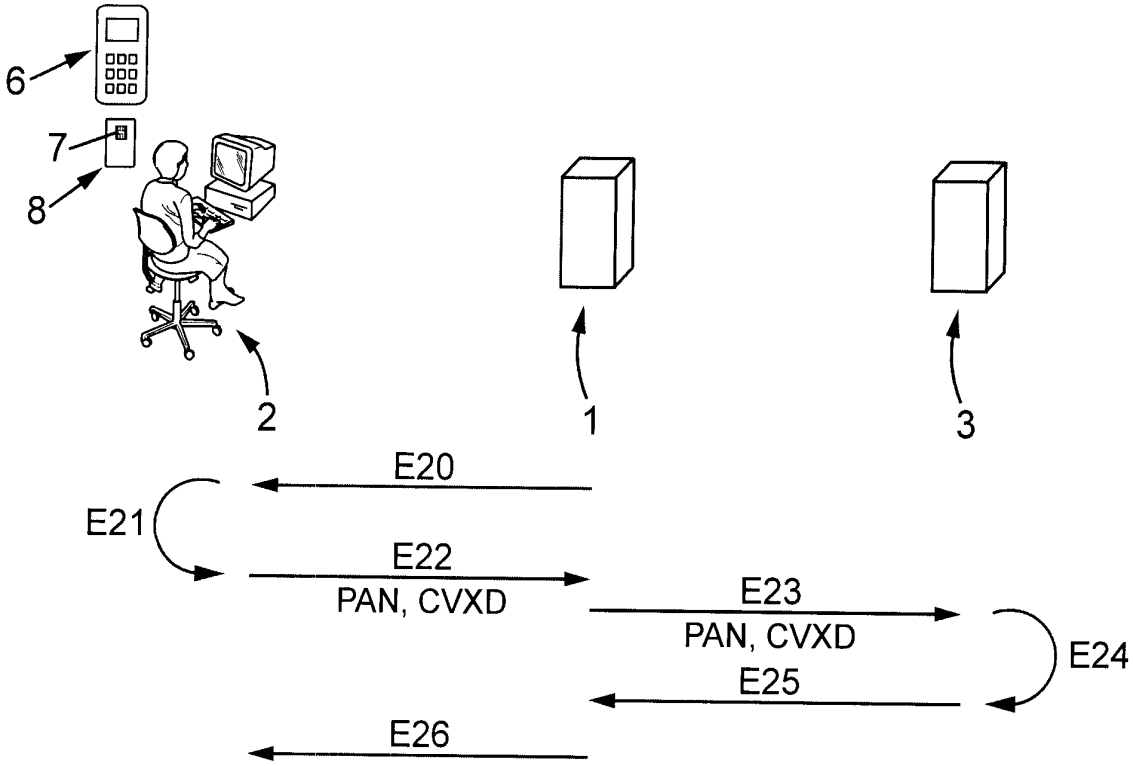

6
7
8
2
1
3
E20
E21
E22
PAN, CVXD
E23
PAN, CVXD
E24
E25
E26

FIG. 3

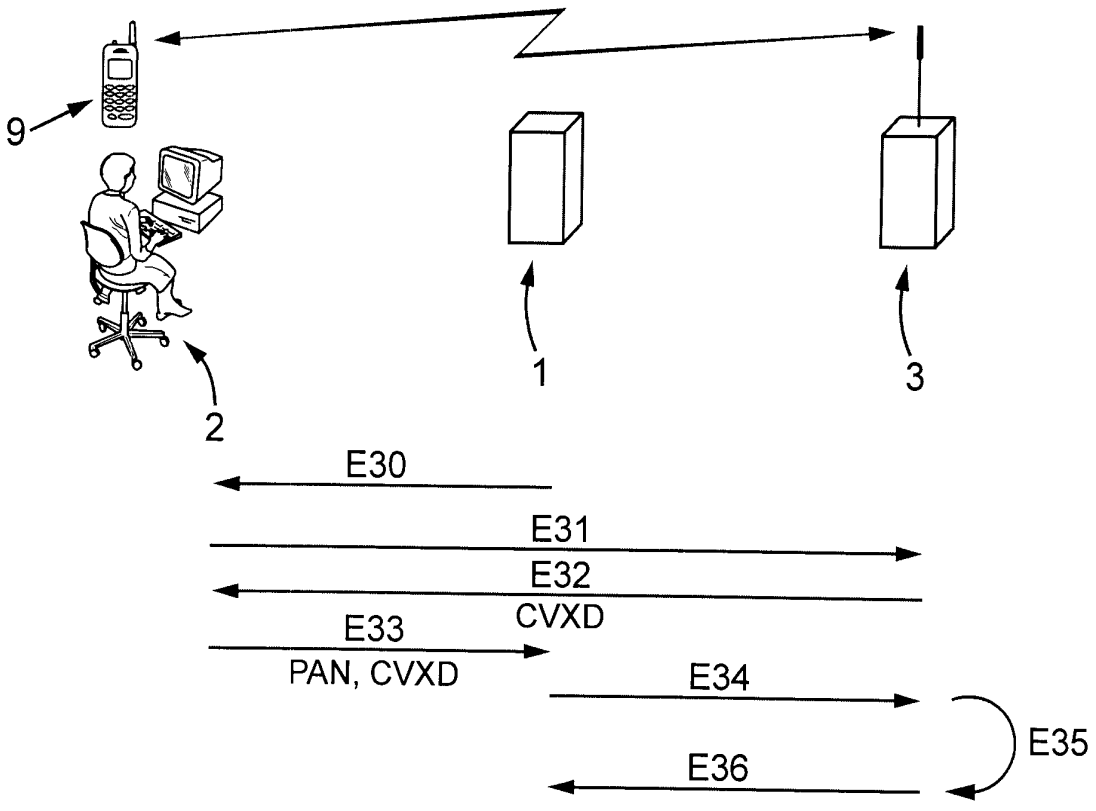

9
1
3
2
E30
E31
E32
CVXD
E33
PAN, CVXD
E34
E35
E36

FIG. 4

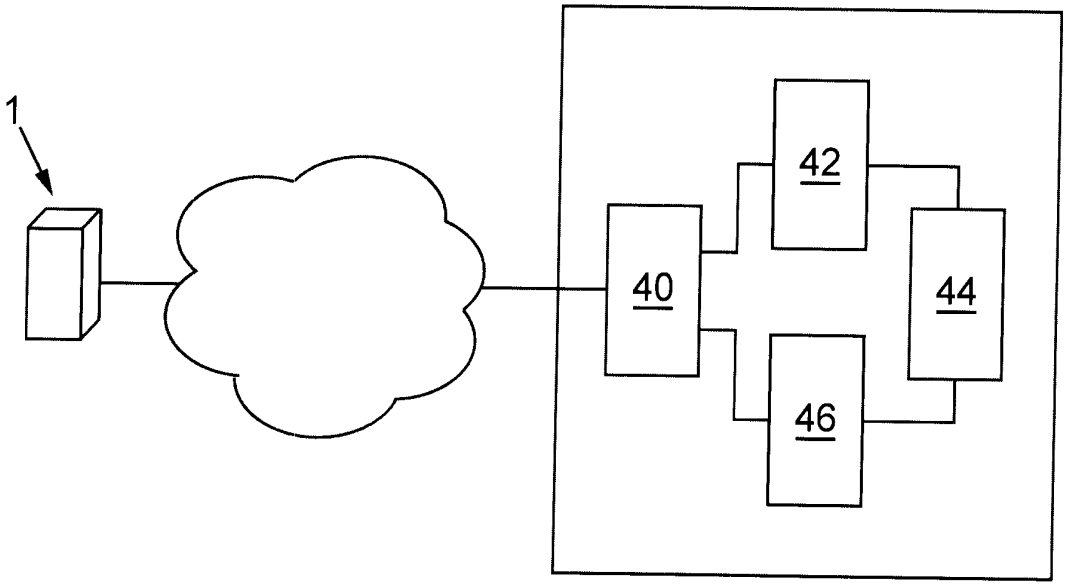


FIG. 5

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 693271
FR 0702551

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		
X	WO 03/073389 A (MASTERCARD EUROP SPRL [BE]; ATES FIKRET [BE]) 4 septembre 2003 (2003-09-04) * page 14, ligne 1 - page 28, ligne 4 * * page 55 - page 57; revendications 1-3; figures 5-8 *	1-11	G06Q20/00
X	WO 2004/109610 A (ZINGTECH LTD [IE]; KIDD SAMUEL ROBERT [NZ]; KIDD MURRAY [NZ]; COPPINGE) 16 décembre 2004 (2004-12-16) * page 2, ligne 1 - page 9, ligne 15 *	1-11	
X	US 6 038 551 A (BARLOW DOUG [US] ET AL) 14 mars 2000 (2000-03-14) * colonne 5 - colonne 18 *	1-11	
X	US 2003/120925 A1 (ROSE GREGORY G [AU] ET AL ROSE GREGORY G [AU] ET AL) 26 juin 2003 (2003-06-26) * le document en entier *	1-11	
X	FR 2 787 273 A1 (SAGEM [FR]) 16 juin 2000 (2000-06-16) * le document en entier *	1-11	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q
X	WO 01/99070 A (MASTERCARD INTERNAT INC [US]) 27 décembre 2001 (2001-12-27) * le document en entier *	1-11	
A	EP 1 229 424 A (CHRYSALIS ITS INC [CA]) 7 août 2002 (2002-08-07) * abrégé *	1-11	
A	EP 1 465 092 A1 (CULTURE COM TECHNOLOGY MACAU L [CN]) 6 octobre 2004 (2004-10-06) * abrégé *	1-11	

-/--

1

Date d'achèvement de la recherche	Examinateur
22 octobre 2007	Lavin Liermo, Jesus

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

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 693271
FR 0702551

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	WO 02/11091 A (VERISIGN INC [US]) 7 février 2002 (2002-02-07) * figure 4b * -----	1-11	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
22 octobre 2007	Lavin Liermo, Jesus

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

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0702551 FA 693271

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 22-10-2007
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 03073389	A	04-09-2003	AU	2003209860 A1	09-09-2003
			BR	0308111 A	04-01-2005
			EP	1479052 A2	24-11-2004
			JP	2005519375 T	30-06-2005
			MX	PA04008410 A	17-05-2005
			US	2005119978 A1	02-06-2005
			ZA	200406805 A	12-09-2005
WO 2004109610	A	16-12-2004	EP	1629442 A1	01-03-2006
US 6038551	A	14-03-2000	US	6810479 B1	26-10-2004
US 2003120925	A1	26-06-2003	AU	2002364095 A1	15-07-2003
			CN	1620779 A	25-05-2005
			EP	1464138 A1	06-10-2004
			JP	2005514831 T	19-05-2005
			WO	03056745 A1	10-07-2003
FR 2787273	A1	16-06-2000	AT	257260 T	15-01-2004
			DE	69913929 D1	05-02-2004
			DE	69913929 T2	23-12-2004
			EP	1014317 A1	28-06-2000
			ES	2209359 T3	16-06-2004
			US	6847816 B1	25-01-2005
WO 0199070	A	27-12-2001	AU	781671 B2	02-06-2005
			AU	7001101 A	02-01-2002
			CA	2382696 A1	27-12-2001
			EP	1320839 A2	25-06-2003
			JP	2003536180 T	02-12-2003
EP 1229424	A	07-08-2002	US	2002104004 A1	01-08-2002
EP 1465092	A1	06-10-2004	AT	316274 T	15-02-2006
			DE	60303234 T2	28-09-2006
WO 0211091	A	07-02-2002	AT	352082 T	15-02-2007
			AU	7794301 A	13-02-2002
			CA	2417406 A1	07-02-2002
			DE	60126096 T2	18-10-2007
			EP	1307863 A1	07-05-2003
			ES	2275702 T3	16-06-2007
			US	2002161721 A1	31-10-2002

EPO FORM P0465