(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 mars 2002 (21.03.2002)

PCT

(10) Numéro de publication internationale
WO 02/23497 A1

(51) Classification internationale des brevets[7] :
G07F 19/00, G06F 17/60

(21) Numéro de la demande internationale :
PCT/FR01/01912

(22) Date de dépôt international : 19 juin 2001 (19.06.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/11828 15 septembre 2000 (15.09.2000) FR

(71) Déposants et
(72) Inventeurs : **POURBAGHER, François** [FR/FR]; 35, quai de Grenelle, F-75015 Paris (FR). **LAVAUR, Richard** [FR/BE]; 97, rue de la source, B-1060 Bruxelles (BE).

(74) Mandataires : **FRECHEDE, Michel** etc.; Cabinet Plasseraud, 84, rue d'Amsterdam, F-75440 Paris Cedex 9 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

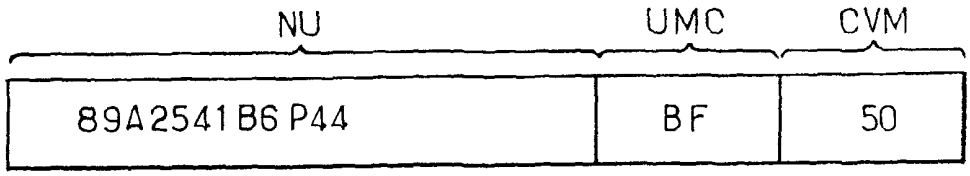
(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** ELECTRONIC NOTE OF FIDUCIARY VALUE, PROTOCOL FOR PAYMENT OF ELECTRONIC COMMERCE PURCHASES AND CORRESPONDING SERVER SYSTEM

(54) **Titre :** BILLET ELECTRONIQUE DE VALEUR FIDUCIAIRE, PROTOCOLE DE PAIEMENT D'ACHATS PAR COMMERCE ELECTRONIQUE ET SYSTEME SERVEUR CORRESPONDANT



NU...NUMBER
UMC...CURRENCY VALUE UNIT
CVM...EQUIVALENT MONETARY VALUE

(57) **Abstract:** The invention concerns an electronic note of fiduciary value comprising at least a field (NU) representing a single number representing an equivalent monetary value (CVM) expressed in a currency value unit (UMC). The single number (NU) is based on the monetary value of the electronic note. The invention is applicable to electronic commerce by anonymous exchange of electronic notes.

(57) **Abrégé :** L'invention concerne un billet électronique de valeur fiduciaire comprenant au moins un champ (NU) représentatif d'un numéro unique représentatif d'un numéro unique représentatif d'une contre-valeur monétaire (CVM) établie en une unité monétaire de compte (UMC). Le numéro unique (NU) est fonction de la valeur monétaire du billet électronique. Application du commerce électronique par échange anonyme de billets électroniques.

WO 02/23497 A1

BILLET ELECTRONIQUE DE VALEUR FIDUCIAIRE, PROTOCOLE DE PAIEMENT D'ACHATS PAR COMMERCE ELECTRONIQUE ET SYSTEME SERVEUR CORRESPONDANT.

L'invention concerne un billet électronique de valeur fiduciaire, un protocole de paiement d'achats par commerce électronique, au moyen d'un ou plusieurs de ces billets, et un système serveur correspondant.

L'avènement, récent, du commerce électronique laisse présager des perspectives de développement très important du volume des transactions réalisées par commerce électronique, dans un avenir proche.

Un obstacle à un tel développement semble résider dans le manque de souplesse, au moins apparent, du paiement des transactions sur les produits ou services proposés.

A l'heure actuelle, le paiement des transactions précitées est réalisé, de manière quasi exclusive, par l'intermédiaire du système des cartes bancaires.

Une carte bancaire est, de manière générale, une carte à microprocesseur, encore désignée carte à puce, à laquelle sont attribués, outre un code confidentiel d'accès à quatre chiffres , un numéro de carte, comportant généralement un ensemble de chiffres, 16 chiffres le plus souvent.

Le numéro de la carte est, bien entendu, associé à un compte bancaire ouvert au nom du titulaire, ce compte bancaire pouvant faire d'ailleurs l'objet de dépôts ou de retraits par le titulaire, indépendamment de l'utilisation de la carte.

Le code confidentiel d'accès permet au détenteur de la carte, titulaire ou non du compte bancaire, d'effectuer toute opération de retrait d'argent liquide à partir notamment de terminaux bancaires désignés par terminaux DAB distributeurs automatiques de billets.

Dans un passé récent, le titulaire de la carte, et du compte bancaire, était en outre en mesure de régler directement tout achat de produits ou service par simple mention sur le document d'achat-vente du numéro de carte bancaire et apposition de sa signature personnelle manuscrite, le compte bancaire du titulaire étant débité du montant de la transaction sur la base de ce document.

Une telle pratique tend à disparaître sous l'impulsion de l'avènement du commerce électronique en raison de l'impossibilité matérielle de réaliser l'appositon de la signature personnelle manuscrite sur un document d'achat-vente.

Sous la pression de l'attrait du commerce électronique, les procédures de signature électronique de documents, notamment de documents d'achat-vente, n'étant à l'heure actuelle pas encore totalement admises par les législations nationales ou considérées trop lourdes pour la majorité des transactions, une pratique de règlement des transactions de commerce électronique s'est développée, laquelle consiste pour le titulaire de la carte, acheteur, à communiquer au vendeur son numéro de carte bancaire.

De convention expresse entre le vendeur et l'acheteur, et bien entendu les organismes bancaires gestionnaires des comptes bancaires de l'acheteur et du vendeur, la communication du numéro de carte bancaire de

l'acheteur au vendeur vaut autorisation à ce dernier de mise en recouvrement du montant de la transaction auprès du gestionnaire de compte bancaire de l'acheteur.

Une telle pratique présente toutefois un inconvénient majeur inhérent à la nature humaine.

L'interception du numéro de carte bancaire par des tiers peu scrupuleux, au cours de la communication de ce numéro au vendeur, permet à ces derniers de faire honorer toute transaction fictive, au préjudice du titulaire de la carte bancaire et du compte bancaire qui lui est associé.

Alors que dans beaucoup de cas, l'honnêteté et l'intégrité du vendeur ne peuvent être suspectées, certains vendeurs indélicats peuvent toutefois être tentés d'utiliser le numéro de carte bancaire communiqué à d'autres fins que le seul paiement de la transaction réalisée.

Enfin, même en dehors de toute utilisation frauduleuse, la détention même licite par un vendeur d'un certain nombre de numéros de cartes bancaires de clients en vue de ou ayant servi à réaliser des transactions expose ces derniers à des risques de piratage par intrusion sur le site du vendeur.

Les risques d'utilisation frauduleuses d'un numéro de carte bancaire, lien direct avec le compte bancaire du titulaire de celle-ci, communiqué en réseau sont donc réels et non négligeables, même en présence d'une communication sécurisée.

La présente invention a pour objet de remédier aux inconvénients précités par la mise en œuvre d'un moyen de paiement électronique dans lequel toute référence et toute

communication de lieu au compte bancaire du possesseur de ce moyen de paiement est supprimé.

En conséquence, un autre objet de la présente invention est la mise en œuvre d'un billet électronique de valeur fiduciaire comportant les attributs sensiblement comparables à ceux d'un billet en papier-monnaie.

Un autre objet de la présente invention est également la mise en œuvre d'un billet électronique de valeur fiduciaire présentant un niveau de confiance comparable ou supérieur à celui d'un billet en papier-monnaie.

Un autre objet de la présente invention est, en conséquence, la mise en œuvre d'un protocole de paiement d'achats de produits ou de services par commerce électronique par échange de billets électroniques conformes à l'objet de la présente invention, en l'absence de toute référence ou de tout lien à l'identité de l'acheteur ou à un compte bancaire dont ce dernier est titulaire.

Un autre objet de la présente invention est, également, la mise en œuvre d'un serveur gestionnaire de transactions réalisées au moyen de billets électroniques conformes à l'objet de la présente invention, ce serveur, placé sous l'autorité de toute entité d'émission habilitée, permettant la mise en œuvre du protocole de paiement d'achats, objet de l'invention, selon une procédure sensiblement équivalente à celle du simple échange de billets en papier-monnaie.

Un autre objet de la présente invention est, enfin la mise en œuvre d'un terminal d'accès en réseau, réseau étendu et/ou réseau local, permettant la mise en œuvre du

protocole de paiement d'achats de produits ou de services par commerce électronique par échange de billets électroniques conformes à l'objet de la présente invention.

Le billet électronique de valeur fiduciaire, objet de la présente invention, est remarquable en ce qu'il comprend au moins un champ représentatif d'un numéro unique représentatif d'une contre-valeur monétaire établie dans une unité monétaire de compte par une entité d'émission.

Le système serveur gestionnaire de transactions réalisées au moyen de billets électroniques de valeur fiduciaire, objet de la présente invention, ces transactions étant réalisées entre un acheteur et un vendeur, est remarquable en ce qu'il comporte au moins un module de mémorisation d'un ensemble de vendeurs accrédités, habilités à conclure une ou plusieurs transactions au moyen de ces billets électroniques, un module de mémorisation de listes de billets électroniques émis valides respectivement invalides, pendant une durée de viduité, un module de contrôle et d'authentification d'accès à ce système serveur de tout vendeur accrédité en vue d'une opération de mise en recouvrement de billets électroniques de valeur fiduciaire échangés au cours d'au moins une transaction, un module de vérification de la validité du numéro unique de chaque billet électronique échangé à partir d'au moins une liste des billets électroniques émis valides et un module de notification au vendeur accrédité d'un message de validation de transaction entre le vendeur et un acheteur quelconque permettant l'envoi au vendeur d'un message de validation

de transaction, sur vérification positive de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé.

Le protocole de paiement d'achats de produits ou de services par commerce électronique entre un terminal client et un terminal vendeur de produits ou services, ce terminal client étant détenteur de billets électroniques de valeur fiduciaire distribués par un organisme serveur spécifique entité d'émission et mémorisés dans ce terminal client, conformes à l'objet de la présente invention, ce terminal vendeur étant géré et contrôlé par un vendeur agréé auprès de cet organisme serveur spécifique, est remarquable en ce que, lors de la conduite d'un accord d'achat/vente de produits ou services pour un prix déterminé, ce protocole consiste au moins à transmettre, à titre de paiement de transaction du terminal client au terminal vendeur un ensemble de billets électroniques dont la somme de la valeur faciale couvre le prix d'achat déterminé, à transmettre du terminal vendeur à l'organisme serveur spécifique cet ensemble de billets électroniques support de cette transaction pour authentification, et, sur procédure d'authentification réussie, à chaque billet électronique de cet ensemble de billets électroniques support de cette transaction étant reconnue la valeur faciale qui lui est dévolue, à transmettre de l'organisme serveur spécifique au terminal vendeur un message de validation de paiement, à invalider au moins, au niveau de cet organisme serveur spécifique, tout billet électronique de cet ensemble de billets électroniques support de cette transaction pendant un délai de viduité, et, sur procédure d'authentification non réussie, à transmettre de

l'organisme serveur spécifique à ce terminal vendeur un message d'invalidation de paiement et de non validation de la transaction.

Le billet électronique de valeur fiduciaire, le système serveur gestionnaire de transactions réalisées au moyen de ces billets électroniques et le protocole de paiement d'achats de produits ou de services par commerce électronique correspondant, objets de la présente invention, trouvent application à toute opération de transaction en ligne par commerce électronique telle que, notamment, paiement d'un prix de cession fixé par contrat, achat d'objets de grande diffusion, souscription d'abonnements ou autres.

Ils seront mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels :

- la figure 1a, représente, à titre illustratif, un billet électronique de valeur fiduciaire, conforme à l'objet de la présente invention, réalisé sous forme de message électronique ;
- les figures 1b et 1c représentent, à titre illustratif, différentes variantes de réalisation du billet électronique de valeur fiduciaire, objet de l'invention tel que représenté en figure 1a ;
- la figure 2a représente, à titre illustratif, un mode de réalisation spécifique d'un billet électronique conforme à l'objet de la présente invention dans lequel le champ relatif à un numéro unique représentatif d'une contre-valeur monétaire est constitué par une valeur chiffrée de longueur quelconque, en fonction du numéro unique représentatif de cette contre-valeur monétaire

et d'autres champs de ce même billet électronique et/ou de variables externes ;

- la figure 2b représente, à titre illustratif, un autre mode de réalisation spécifique d'un billet électronique conforme à l'objet de l'invention dans lequel le champ relatif à un numéro unique représentatif d'une contre-valeur monétaire, est constitué par une valeur de signature électronique de longueur fixe, cette valeur de signature étant établie à partir de ce numéro unique et d'une pluralité d'autres champs de ce même billet électronique et/ou de variables externes ;
- la figure 2c représente, à titre illustratif, un mode opératoire permettant l'obtention de la valeur chiffrée de longueur quelconque du billet électronique représenté en figure 2a par chiffrement à partir d'une clé secrète ;
- la figure 2d représente, à titre illustratif, un mode opératoire permettant à l'entité d'émission d'opérer sur tout billet électronique de son choix, tel que représenté en figure 2a, une opération d'authentification de non répudiation grâce à une opération de déchiffrement à partir de la clé secrète utilisée lors du chiffrement ;
- la figure 2e représente, à titre illustratif, un mode opératoire permettant l'obtention de la valeur de signature de longueur fixe du billet électronique représenté en figure 2b par signature à partir d'une clé de signature ;
- -la figure 2f représente, à titre illustratif, un mode opératoire permettant à l'entité d'émission d'opérer sur tout billet électronique de son choix, tel que

représenté en figure 2b, une opération d'authentification et de non répudiation grâce à une opération de déchiffrement à partir d'une clé de vérification de signature, distincte de la clé de signature ;

- la figure 3a représente, à titre illustratif, un schéma synoptique relatif à un serveur gestionnaire de transactions réalisées au moyen de billets électroniques conformes à l'objet de la présente invention ;
- la figure 3b représente, à titre illustratif, un organigramme fonctionnel du serveur gestionnaire objet de l'invention tel que représenté en figure 3a ;
- la figure 4a représente, à titre illustratif, un organigramme relatif à un protocole de paiement d'achats de produits ou services par commerce électronique entre un terminal client et un terminal vendeur, conforme à l'objet de la présente invention ;
- la figure 4b représente, à titre illustratif, une variante de mise en œuvre du protocole de paiement objet de la présente invention de la figure 4a dans lequel une mesure de sécurité consistant à inhiber temporairement l'utilisation ultérieure de billets électroniques, suite à une première utilisation est introduite ;
- la figure 4c représente, à titre purement illustratif, une variante de mise en œuvre du protocole de paiement objet de la présente invention dans lequel une mesure de sécurité est introduite, suite à la réception par le terminal client d'un message d'accusé de réception de validation de la transaction, par l'intermédiaire du

terminal vendeur, l'ensemble des billets électroniques, support de la transaction, étant effacé dans ce terminal client ;

- la figure 4d représente, à titre illustratif, un exemple de mise en œuvre spécifique de l'introduction , par l'entité d'émission, au niveau du serveur gestionnaire, d'un délai de viduité pour un ou plusieurs billets électroniques, supports d'une transaction, ce délai de viduité consistant en une invalidation simplement interne au serveur du ou des billets électroniques, pendant leur durée de validité, en l'absence de mise en recouvrement de ce ou de ces billets électroniques par leur détenteur, ce délai de viduité consistant au contraire en une invalidation interne au niveau du serveur et externe à ce serveur de ce ou de ces billets électroniques pendant un délai de viduité très supérieur à la durée de validité de ce ou de ces billets électroniques. ;
- la figure 5 représente, à titre illustratif, une variante non limitative de mise en œuvre du protocole, objet de l'invention dans laquelle une procédure de rendu de monnaie est introduite.

Une description plus détaillée d'un billet électronique de valeur fiduciaire conforme à l'objet de la présente invention sera maintenant donnée en liaison avec les figures 1a, 1c, 2a à 2f.

D'une manière générale, on indique que le billet électronique de valeur fiduciaire, objet de la présente invention, est mis en œuvre sous forme d'un message ou d'un fichier électronique destiné à un échange entre terminaux et/ou serveur et, de manière plus particulière,

dans le cadre d'une transaction entre un terminal client, noté TC, et un terminal vendeur pouvant, le cas échéant, être constitué par un serveur, noté TV.

En référence à la figure 1a, on indique que selon un aspect particulièrement remarquable du billet électronique, objet de la présente invention, celui-ci comprend, au moins, un champ représentatif d'un numéro unique. Ce numéro unique étant lui-même représentatif d'une contre-valeur monétaire établie dans une unité monétaire de compte par une entité d'émission.

Sur la figure 1a, le champ représentatif du numéro unique est noté NU. Il peut être associé à un champ de contre-valeur monétaire, noté CVM et à un champ d'unité monétaire de compte, noté UMC.

En ce qui concerne la notion d'entité d'émissions, on indique que dans le cadre de mise en œuvre des billets électroniques de valeur fiduciaire, du système serveur gestionnaire de transactions réalisées au moyen de billets électroniques de valeur fiduciaire correspondants et du protocole de paiement d'achats de produits ou de services par commerce électronique entre terminal client et un terminal vendeur de produits ou services, conformément à l'objet de la présente invention, concerne tout organisme, toute société commerciale et/ou financière habilitée par les autorités d'un Etat souverain ou d'un groupe d'Etats souverains à émettre et à distribuer des billets électroniques conformes aux billets électroniques, objets de la présente invention.

D'une manière générale, on indique que le champ NU, représentatif d'un numéro unique est avantageusement constitué par un ensemble de caractères alphanumériques.

Le nombre de caractères alphanumériques de cet ensemble de caractères alphanumériques peut avantageusement être fonction de la contre-valeur monétaire CVM attribuée aux numéros uniques NU correspondants.

Dans un exemple de mise en œuvre spécifique non limitatif et pour une unité monétaire de compte telle que le franc français, un billet dont la contre-valeur monétaire, c'est à dire la valeur faciale, est établie à 50 F comporte un numéro unique NU comprenant douze caractères alphanumériques, un billet de valeur faciale 100 FF peut comprendre avantageusement un numéro unique comprenant 15 caractères alphanumériques et un billet électronique de valeur faciale 500 F peut comprendre avantageusement un numéro unique NU comportant 18 caractères alphanumériques.

Bien entendu, le billet électronique, objet de la présente invention peut être muni de différents champs auxiliaires lesquels seront explicités ultérieurement dans la description.

Dans un mode de réalisation non limitatif ainsi que représenté en figure 1a ou 1b, le billet électronique objet de la présente invention peut être mis en œuvre à partir d'un numéro unique NU constitué par un ensemble de caractères alphanumériques comportant au moins un nombre déterminé de digits (un digit désigne un chiffre ou une lettre) fonction de la contre-valeur monétaire attribuée au numéro monétaire unique. Ces digits étant représentatifs d'un nombre unique lié à la contre-valeur monétaire précitée.

En outre, un nombre déterminé de caractères alphanumériques inférieur au nombre de digits peut être

prévu. Un ou plusieurs caractères alphanumériques étant insérés entre deux digits.

Sur la figure 1a, on a représenté un billet électronique de contre-valeur monétaire CVM égal à 50 pour une unité monétaire de compte UMC exprimé par un code tel que le code BF pour des francs français par exemple. Le numéro unique NU étant constitué par une suite de caractères alphanumériques : 8, 9A, 254, 1B6, P44 par exemple.

Dans ces conditions, un billet de 50 F par exemple est représenté par une série de douze caractères plus un ou plusieurs champs auxiliaires spécifiant l'unité monétaire de compte, c'est à dire la monnaie, ainsi qu'il sera décrit ultérieurement dans la description.

Dans ces conditions, le numéro unique NU formé par les douze caractères alphanumériques est composé de neuf chiffres et trois lettres. Les trois lettres ou caractères alphanumériques étant choisis parmi les vingt-six lettres de l'alphabet européen ou, le cas échéant, les 256 caractères ASCII par exemple. Des caractères alphanumériques peuvent être placés au hasard à des emplacements de position aléatoire entre deux digits successifs du nombre déterminé fonction de la contre-valeur monétaire attribuée au numéro unique.

Les neufs digits précités procurent déjà un milliard de possibilités dans le choix d'un numéro unique spécifique attribué à la contre-valeur monétaire correspondante. Les caractères alphanumériques permettent d'effectuer 17 576 combinaisons différentes et en raison de l'emplacement aléatoire des caractères précités entre deux digits successifs, on obtient ainsi un facteur de

1 320 combinaisons supplémentaires en raison du placement des caractères alphanumériques précités dans la série de digits précités.

Pour le codage d'une première contre-valeur monétaire CVM de 50 F par exemple, on dispose ainsi d'un nombre de possibilités correspondant :

à 1 000 000 000 x 17 576 caractères alphanumériques
x 1 320 positions pour ces caractères, soit
23 200 320 milliards de combinaisons de chiffrages différents.

Si l'on suppose donc que l'entité d'émission ne valide qu'une combinaison sur les vingt-trois millions, il est alors possible, pour cette dernière, de mettre en circulation 50 000 000 000 de francs français sous forme de monnaie virtuelle en billets électroniques par l'intermédiaire de coupures de 50 F.

Il est bien entendu que toute autre unité monétaire de compte UMC peut être utilisée en fonction de l'autorisation reçue par les autorités nationales ou régionales contrôlant l'émission des valeurs fiduciaires.

Pour retrouver la bonne combinaison, un faussaire doit, non seulement, pouvoir essayer 23 millions de combinaisons en moyenne pour un billet de valeur faciale 50 F mais, en outre, satisfaire au critère de contrôle strict, d'authentification et de non répudiation de billets imposé par l'entité d'émissions et en particulier par tout serveur, gestionnaire de transactions réalisées au moyen de billets électroniques, objets de la présente invention dans le cadre d'un protocole spécifique, lesquelles seront décrites ultérieurement dans la description.

Sur la figure 1b, on a représenté différents modes de réalisation de billets électroniques conformes à l'objet de la présente invention pour différentes valeurs, de contre-valeurs monétaires et donc de valeurs faciales de ces billets électroniques.

Le premier exemple de billet électronique représenté en figure 1b reprend l'exemple donné en figure 1a pour un billet de valeur faciale 50 F.

Le deuxième exemple de billet électronique représenté en figure 1b correspondant à celui d'un billet électronique de valeur faciale 100 F par exemple. Dans ce cas, et pour la valeur faciale c'est à dire la contre-valeur monétaire CVM est égale à 100 F, le numéro unique NU peut comporter 15 caractères alphanumériques c'est à dire 12 digits et 03 caractères alphanumériques par exemple. Sur la figure 1b dans le deuxième exemple, le numéro unique NU s'écrit :

585 / 46A / 222 / R48 / W12.

On dispose dans ces conditions de mille milliards de combinaisons en raison de l'existence de 12 digits, ce nombre de combinaisons étant multiplié par 26^3 = 17 576 combinaisons pour les 03 caractères alphanumériques et encore multiplié par 15 x 14 x 13 = 2 730 combinaisons pour la position aléatoire des caractères alphanumériques entre les digits précités c'est à dire un total de 47 982 480 fois mille milliards.

Dans ces conditions, l'entité d'émission a donc la possibilité d'émettre en unité monétaire de compte 47 982 480 fois mille milliards X 100 unités monétaires de compte

c'est à dire francs français dans l'exemple représenté au deuxième exemple de la figure 1b.

Ainsi, l'entité d'émission peut choisir un chiffre valide correspondant au numéro unique NU représenté au deuxième exemple de la figure 1b à partir duquel l'entité d'émission pourrait émettre 100 000 000 000 000 (cent mille milliards) d'unités monétaires de compte UMC c'est à dire de francs dans l'exemple retenu. Un faussaire doit, par contre, effectuer 47 000 000 de combinaisons pour trouver la combinaison correspondante.

Dans le troisième exemple de la figure 1b, on a représenté, pour un billet de 500 F, un nombre de 15 digits auxquels sont ajoutés 03 caractères alphanumériques.

A titre d'exemple dans l'imitative, le troisième exemple de la figure 1b comporte un numéro unique NU représenté par :

T52 / 562 / 789 / GH1 / 459 / 770.

Dans ces conditions, il existe pour l'entité d'émission 1 million de milliards de combinaisons en chiffres x 26^3 = 17 576 caractères alphanumériques placés indifféremment soit en fait 18 x 17 x 16 = 4 896 combinaisons de placement différentes pour un nombre total de combinaisons de 86 052 096 de combinaisons différentes de 1 000 000 de milliards.

Pour assurer la mise en correspondance bi-univoque entre un billet et la valeur faciale ou contre-valeur monétaire qui est associée au numéro unique de celui-ci, l'entité d'émission dispose, par exemple, d'un algorithme de choix aléatoire entre l'une des combinaisons précitées

et la valeur faciale allouée à la combinaison retenue permet d'assurer la mise en correspondance bi-univoque entre l'une des combinaisons, fonction du nombre déterminé de digits du nombre de caractères alphanumériques et de la position relative de ces derniers par rapport aux digits et de la valeur faciale ou contre-valeur monétaire attribuée à cette combinaison.

L'algorithme précité est, de préférence, un algorithme non linéaire lequel, grâce à un tirage aléatoire, permet d'assurer la mise en correspondance bi-univoque précitée.

Dans ces conditions, le tableau ci-après indique les capacités d'émission pour l'entité d'émission exprimées pour chaque valeur faciale c'est à dire chaque contre-valeur monétaire CVM en nombre de billets maximum émissibles pour un nombre de caractères alphanumériques entre parenthèses et en masse monétaire virtuelle disponible ainsi que représenté ci-après :

CVM VALEUR FACIALE	NOMBRE DE BILLETS VIRTUELS MAXIMUM	MASSE MONETAIRE VIRTUELLE MAXIMUM	PRC/F
50 UMC	(12) 23 200 320 milliards	50 000 000 000 UMC	1/23 millions
100 UMC	(15) 47 982 480 x 1 000 milliards	100 000 000 000 000 UMC	1/47 millions
500 UMC	(18) 86 052 096 x 1 million de milliards	500 000 000 000 000 UMC	1/86 millions

Dans le tableau précité, la valeur faciale de chaque billet virtuel est exprimée en unité monétaire de compte UMC. Il en est de même pour la masse monétaire virtuelle susceptible d'être mise en circulation par

l'entité d'émission, cette unité monétaire de compte étant susceptible, bien entendu, d'être émise et de correspondre à toute unité monétaire de compte telle que le franc, le dollar, l'euro ou autre unité monétaire de compte légal.

En outre, dans le tableau précité, la dernière colonne représente la probabilité de découverte de la combinaison pour un faussaire par exemple, compte tenu des indications données en liaison avec les figures 1a et 1b . Cette probabilité est notée Prc/f.

Sur la facture 1c, on a représenté un billet électronique de valeur fiduciaire conforme à l'objet de la présente invention comportant, bien entendu, les champs précédemment décrits en liaison avec les figures 1a et 1b mais également au moins un champ auxiliaire noté EE, représentatif de l'entité d'émission, ce champ étant noté EE et étant réputé correspondre à un code d'identification d'une banque ou de toute société habilitée à jouer le rôle d'une entité d'émission, ainsi qu'un champ auxiliaire représentatif du pays hôte de cette entité d'émission. Dans le cas de la figure 1c, l'exemple non limitatif correspond à une banque en France, la BNP, le pays étant la France, notée FR.

Enfin, ainsi que représenté en figure 1c, le billet électronique de valeur fiduciaire, objet de la présente invention peut comporter, de manière particulièrement avantageuse, en outre, un champ auxiliaire représentatif de la durée de validité du billet électronique précité. Ce champ est noté DV sur la figure 1c. Il peut comprendre une valeur de date d'émission du billet électronique par l'entité d'émission, valeur notée X et une valeur Y de date de fin de la validité du billet

électronique considéré. Les valeurs X et Y peuvent être exprimées de manière classique en années YY, mois MM, jour DD, heure HH, minute mn et seconde ss.

Selon une caractéristique avantageuse de chaque billet électronique, objet de la présente invention, la durée de validité de ces derniers peut être modulée en fonction de la valeur faciale c'est à dire de la contre-valeur monétaire CVM allouée à chacun de ces derniers. Ainsi,

- pour des billets de valeur faciale peu élevée c'est à dire inférieure à 50 unités monétaires de compte, par exemple 50 F, la durée de validité DV peut être établie à deux mois par exemple ;
- pour des billets électroniques de valeur faciale moyenne comprise entre 50 et 500 unités monétaires de compte, la durée de validité DV peut être établie à un mois ;
- pour des billets électroniques de valeur faciale supérieure à 500 F, UMC, la durée de validité DV peut être réduite à 3 jours par exemple.

On comprend, en particulier, que la faible durée allouée aux billets électroniques de valeur faciale la plus élevée permet de réduite le risque d'interception et de décodage des numéros uniques associés à chacun d'eux lors de la transmission de ces derniers sur le réseau par des utilisateurs indélicats dans un temps raisonnable, alors que la durée de validité plus importante allouée aux billets électroniques de valeur la plus faible permet d'utiliser ceux-ci pendant cette durée à des fins d'échanges de manière très semblable à des billets en

papier-monnaie, ainsi qu'il sera décrit ultérieurement dans la description.

D'une manière générale, on indique que les billets électroniques, objets de la présente invention, sont destinés à être utilisés par tout utilisateur qui en a fait régulièrement l'acquisition auprès de l'entité d'émission dans des conditions qui seront explicitées ultérieurement dans la description.

A ce titre, et de manière non limitative, on indique que chaque billet électronique outre le numéro unique NU, peut comporter avantageusement, en clair, la valeur faciale du billet ou contre-valeur monétaire CVM, l'unité monétaire de compte correspondante UMC, l'entité d'émission EE et, bien entendu, le pays hôte de l'entité d'émission par exemple.

Toutefois, et afin de sécuriser non plus le billet en tant que tel c'est à dire le numéro unique NU mais toute transaction réalisée à partir d'un billet ou d'un ensemble de billets électroniques, objets de la présente invention, toute information c'est à dire tout champ du billet électronique, objet de l'invention autre que les champs précédemment cités contenant des informations en clair, peut avantageusement être constitué par une valeur chiffrée ou une valeur de signature non accessible à l'utilisateur habilité et donc au tiers, afin d'assurer une meilleure sécurité des transactions.

Dans ce but, ainsi que représenté en figure 2a, le champ représentatif du numéro unique peut avantageusement être constitué par une valeur chiffrée à partir d'une pluralité de variables du billet électronique comprenant au moins le numéro unique NU, l'entité d'émission EE, la

valeur faciale c'est à dire la contre-valeur monétaire CVM du billet ainsi par exemple que l'unité monétaire de compte UMC.

On comprend en particulier que dans ces conditions, le champ de numéro unique lorsque celui-ci est représenté par une valeur chiffrée est désigné par CNU pour désigner cette valeur.

Ainsi que représenté sur la figure 2a, on indique que le champ relatif au numéro unique chiffré CNU peut représenter une longueur variable c'est à dire non constante pour chaque billet électronique successif en fonction du processus de chiffrement utilisé par l'entité d'émission.

Au contraire, ainsi que représenté en figure 2b, le champ relatif au numéro unique chiffré CNU peut présenter une longueur fixe, c'est à dire constante, quel que soit le type de billet émis lorsqu'un processus de chiffrement spécifique par signature électronique à partir d'une fonction de hachage par exemple est mis en œuvre ainsi qu'il sera décrit ultérieurement dans la description.

En outre, sur la figure 2b, on indique que la valeur faciale du billet peut être constituée par une valeur dédiée, cette valeur dédiée 550,09 unités monétaires de compte ayant été établie à la demande d'un utilisateur, c'est à dire d'un terminal client TC, par l'entité d'émission pour réaliser une transaction particulière dont le montant correspond exactement à la valeur dédiée précitée.

Dans ces conditions, on comprend que le billet électronique objet de la présente invention présente un

degré de sécurité et d'authenticité comparable à celui d'un chèque de banque certifié pour le montant correspondant à la valeur des billets précités. On comprend évidemment que la certification de la valeur des billets, et bien entendu du billet électronique porteur de la valeur faciale correspondante, est donnée par l'entité d'émission dans les conditions qui seront décrites ci-après en liaison avec les figures 2c, 2d et 2e, 2f.

D'une manière générale, on indique que l'établissement d'une valeur de numéro unique chiffré CNU de longueur variable peut, par exemple, être obtenue à partir de processus de chiffrement à partir d'une clé secrète notée KS par la technique du masque jetable par exemple ou une technique de stéganographie.

Dans ce but, ainsi que représenté en figure 2c l'on procède à une étape CH1 à une concaténation des champs de numéro utile NU, d'entité d'émission EE, de contre-valeur monétaire CVM, d'unité monétaire de compte UMC pour obtenir une chaîne de caractères notée $.

La concaténation s'entend soit de la concaténation simple des champs précités, soit d'une concaténation dite embrouillée selon un algorithme spécifique de mélange des caractères consécutifs de chaque champ.

En outre et de manière non limitative, aux valeurs des champs du billet électronique précité peut être ajouté au moins un champ externe à celui-ci tel que par exemple l'adresse électronique du terminal créancier c'est à dire du terminal vendeur TV dans l'exemple de transactions précédemment mentionnées dans la description, cette adresse étant notée ATV par exemple.

On comprend en particulier que l'introduction d'un champ de valeur externe telle que l'adresse du terminal vendeur ATV permet de diversifier la longueur du champ du numéro utile chiffré CNU, celui-ci n'étant donc pas de longueur constante en fonction de la longueur de l'adresse du terminal vendeur précité. En outre, l'introduction d'une telle adresse lors de l'exécution d'une transaction permet, d'une part, de justifier de la possession du billet par le terminal créancier c'est à dire le terminal vendeur et par le destinataire c'est à dire par le vendeur agréé suite à une validation de la transaction précitée et, d'autre part, d'assurer un échange sécurisé du même billet électronique au cours de transactions successives par simple remplacement dans la pluralité de variables de l'adresse électronique du terminal vendeur c'est à dire le terminal créancier destinataire de ce billet électronique.

La chaîne de caractères $ ainsi obtenue est alors soumise à une étape CH2 à une opération de chiffrement à partir de la clé secrète KS. Cette opération est notée :

$C = C_{KS}(\$) = CNU$.

Dans la relation précédente $C_{KS}(\$)$ désigne l'opération de chiffrement de la chaîne de caractères dollar et C désigne la valeur chiffrée ainsi obtenue et correspondant à la valeur du champ CNU.

Les opérations précitées permettent à l'entité d'émission d'assurer sur tout billet des opérations d'authentification et de non répudiation que cette dernière juge nécessaires.

Dans ces conditions, sur réception d'un billet comportant un champ de numéro unique chiffré CNU et lorsque ce champ a été obtenu à partir du chiffrement par

l'intermédiaire d'une clé secrète KS, ces opérations, ainsi que représentées en figure 2d, peuvent consister à effectuer un déchiffrement du champ CNU, cette opération étant notée :

$D_{KS}(CNU) \Rightarrow \$$ et permettant de restituer la chaîne de caractères non chiffrés obtenue par l'opération de concaténation précédemment mentionnée en liaison avec la figure 2c. L'opération de déchiffrement DCH1 est alors suivie d'une opération de lecture de la chaîne de caractères dollar, opération notée DCH2, cette opération de lecture permettant de restituer, soit par lecture directe lorsque la concaténation a été effectuée comme une concaténation directe, soit après désembrouillage et lecture lorsque la concaténation a été précédée d'une opération d'embrouillage, de restituer les champs candidats NQ*, EE*, CVM*, UMC* et ATV*. Ces champs candidats étant des champs obtenus de par l'opération de déchiffrement réalisée à l'étape DCH1.

L'entité d'émission procède alors en une étape DCH3 en une comparaison d'égalité de chaque champ candidat NQ*, EE*, CVM*, UMC* avec les champs d'origine non chiffrés NU, EE, CVM, UMC respectivement.

Sur réponse positive à l'ensemble des opérations de comparaison d'égalité réalisées à l'étape DCH3, le billet électronique est authentifié et non répudié par l'entité d'émission à l'étape DCH5.

Au contraire, sur réponse négative à l'une des comparaisons d'égalité réalisées à l'étape DCH3, le billet électronique est invalidé à l'étape DCH4 par l'entité d'émission.

Les figures 2e et 2f concernent des opérations comparables de calcul de signature pour constituer un champ de numéro unique chiffré CNU de longueur fixe tel que représenté en figure 2b.

Pour obtenir un champ de numéro unique correspondant à une valeur de signature de longueur fixe ou constante quel que soit le billet, une telle opération peut être réalisée par le calcul d'une valeur de signature à partir d'une fonction de hachage H ainsi que représentée en figure 2e.

Les valeurs des champs de numéros utiles NU, d'entité d'émission EE, de contre-valeur monétaire CVM, d'unité monétaire de compte UMC et, le cas échéant, de valeurs externes aux billets électroniques tel que l'adresse du terminal vendeur ATV et, par exemple, une variable aléatoire VA peuvent être soumis à une concaténation dans les conditions telles que précédemment mentionnées dans la description à une étape CH3, pour obtenir une chaîne de caractères notée $$.

L'étape de concaténation précitée peut être suivie du calcul par l'intermédiaire d'une fonction de hachage d'une valeur hachée de longueur normalisée fixe, cette opération étant notée :

$$H\ \$\$ \Rightarrow N\$.$$

La chaîne de caractères de longueur normalisée N$ est alors soumise à signature à partir d'une clé privée K_{PR} à partir d'un algorithme tel que l'algorithme RSA par exemple. Cette opération est notée :

$$S = S_{KPR}\ (N\$)$$

pour obtenir la valeur signée, c'est à dire le champ CNU de longueur fixe.

Dans la relation précédente, S désigne la valeur de signature effectivement obtenue et S_{KPR} désigne l'opération de signature à partir de l'algorithme RSA précité et de la clé privée KPR.

Pour réaliser les opérations d'authentification et de non répudiation d'un billet électronique, l'entité d'émission est alors en mesure de procéder ainsi que représenté à la figure 2f.

L'entité d'émission dispose du champ de numéros utiles chiffrés CNU correspondant à la valeur de signature précitée de longueur fixe.

Elle est alors en mesure, en une étape DCH6, de procéder à une vérification de la signature précitée à partir d'une clé de vérification de signature notée KPU, cette clé constituant une clé dissymétrique vis-à-vis de la clé de calcul de signature KPR. L'opération de vérification est effectuée à partir de l'algorithme RSA par exemple et est notée :

$$\mathcal{V}_{KPU}\ (CNU) = \mathcal{V}_{KPU}\ (S_{KPR}\ \{N\$\})$$

Cette opération permet d'obtenir les champs candidats NU*, EE*, CVM*, UMC*, ATV* et bien entendu VA*. L'opération DCH6 est alors suivie d'une opération de vérification par comparaison d'égalité des champs candidats précités NU*, EE*, CVM*, UMC* et VA* par exemple ainsi que, le cas échéant, du champ candidat ATV* aux valeurs de champs d'origine NU, EE, CVM, le cas échéant, VA et ATV.

Sur réponse négative à l'une des comparaisons d'égalité du test BCH7, l'entité d'émission procède à une invalidation à l'étape DCH8. Au contraire, sur réponse positive à toutes les comparaisons d'égalité de l'étape

DCH7, l'entité d'émission procède à une authentification à une non-répudiation du billet électronique considéré à l'étape DCH9.

Une description plus détaillée d'un système serveur gestionnaire de transactions réalisées au moyen de billets électroniques de valeur fiduciaire, conformes à l'objet de la présente invention, sera maintenant décrit en liaison avec les figures 3a et 3b.

D'une manière générale, on indique que les transactions prises en considération interviennent entre un acheteur et un vendeur, ces transactions étant réalisées à partir d'un terminal client acheteur noté TC et un terminal vendeur noté TV, ce terminal vendeur pouvant bien entendu consister en un serveur assurant les opérations de commerce électronique adéquates.

Ainsi que représenté sur la figure 3a, le système serveur comprend un module de mémorisation noté HDD1 d'un ensemble de vendeurs accrédités habilités à conclure une ou plusieurs transactions au moyen des billets électroniques de valeur fiduciaire décrites précédemment dans la description.

D'une manière générale, on indique que le module de mémorisation HDD1 est constitué avantageusement par un disque dur autonome permettant de mémoriser l'ensemble des vendeurs accrédités sous forme d'une liste ou, le cas échéant, d'un tableau, la liste ou le tableau étant constitué par des entités ou des variables correspondant au nom du vendeur, à l'adresse électronique de son terminal et à un code d'accès d'accréditation du vendeur auprès du système serveur gestionnaire de billets

électroniques tels que représentés en figure 1 par exemple.

En outre, le système serveur, objet de l'invention comprend un module noté HDD2 de mémorisation de listes de billets électroniques de valeur fiduciaire émis valides respectivement invalides pendant une durée de viduité.

Dans un mode de réalisation simplifié, le module HDD2 de mémorisation des listes de billets électroniques précités est constitué par un disque dur indépendant permettant de mémoriser ces listes sous forme de listes distinctes comportant au moins le numéro du billet considéré dans un répertoire de billets émis valides respectivement un répertoire de billets émis invalides.

On comprend bien entendu que la réalisation des modules HDD1 et HDD2 sous forme de disque dur indépendant permet d'appliquer des conditions de sécurité d'accès particulièrement draconiennes en ce qui concerne le module HDD2 de mémorisation de listes de billets électroniques valides respectivement invalides. Ces conditions d'accès particulièrement sévères peuvent, le cas échéant, ne pas être appliquées de manière aussi stricte au module de mémorisation HDD1. Les processus de contrôle d'accès correspondants qui peuvent correspondre à des processus de contrôle d'accès classiques ne seront pas décrits en détail dans la description pour cette raison.

En outre, ainsi que représenté en figure 3a, le système serveur, objet de la présente invention comprend un module 1 de contrôle et d'authentification d'accès au système serveur de tout vendeur accrédité en vue d'une opération soit d'authentification de transactions et en particulier d'authentification du paiement réalisé au

moyen d'un ou plusieurs billets électroniques précédemment décrits dans la description, soit de mise en recouvrement de billets électroniques de valeur fiduciaire échangés au cours de cette transaction.

Un protocole simple d'authentification peut consister, sur accès d'un vendeur accrédité présentant son code d'accès, en une comparaison de ce code d'accès vis-à-vis du code d'accès de référence mémorisé dans le module HDD1. Bien entendu, les conditions de mise en œuvre du protocole de contrôle d'accès correspondant à des conditions habituelles compte tenu des règles de sécurité imposées ne sera pas décrit dans la description pour cette raison.

Le système serveur objet de la présente invention comporte également un module 2 de vérification de la validité du numéro unique de chaque billet électronique NU de valeur fiduciaire échangé à partir d'au moins une liste de billets électroniques de valeur fiduciaire valides et invalides. Ce module de vérification 2 peut consister en un module de type module logiciel permettant d'assurer la vérification selon le test de comparaison DCH3 représenté en figure 2d ou DCH7 représenté en figure 2f, en fonction du type de chiffrement ou de calcul de valeur de signature utilisé.

Lorsque les billets électroniques mis en circulation ne comportent pas de champ de numéro unique chiffré, le numéro unique en clair étant seul transmis, l'opération réalisée par le module 2 de vérification de la validité du numéro unique de chaque billet électronique se résume à la comparaison d'égalité des champs candidats

reçus en clair, vis-à-vis des champs de référence lus sur le module de mémorisation HDD2.

Enfin, le système serveur comporte un module 3 de notification au vendeur accrédité, c'est à dire au terminal vendeur TV, d'un message de validation de transaction entre le vendeur et un acheteur quelconque. Ce module 3 permet l'envoi au vendeur d'un message de validation de transaction sur vérification positive de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé, ainsi qu'il a été explicité précédemment dans la description.

Le module 2 de vérification du numéro unique peut, ainsi que représenté en figure 3a, être en outre accompagné d'un module 4 de comptage du nombre d'erreurs de vérification de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé, ainsi que d'un module 5 de comparaison du nombre d'erreurs de vérification de la validité du numéro unique à une valeur de seuil. Sur la figure 3a, les modules 4 et 5 de comptage du nombre d'erreurs et de comparaison du nombre d'erreurs à une valeur de seuil sont représentés par un même élément afin de ne pas surcharger inutilement le dessin.

En ce qui concerne la valeur de seuil précitée, celle-ci peut être contenue et mémorisée sur le module HDD2.

Dans un mode de réalisation particulier le module 4,5 de comparaison permet de piloter le module de notification 3 et permet l'envoi d'un message d'invalidation de transaction au vendeur accrédité lorsque le nombre d'erreur de vérification est supérieur ou égal à la valeur de seuil Vseuil considéré.

Le mode opératoire du serveur représenté en figure 3a sera maintenant décrit en liaison avec la figure 3b. L'entité d'émission qui assure la gestion et le contrôle du système serveur gestionnaire de transaction réalisée au moyen de billets électroniques, conformes à l'objet de la présente invention, contrôle par l'intermédiaire de ce serveur deux tâches principales : celle consistant à valider les numéros uniques présentés et celle consistant à procéder aux opérations bancaires correspondantes.

Chaque vendeur souhaitant proposer le mode de paiement, objet de la présente invention, au moyen des billets électroniques correspondants, doit au préalable remplir un dossier d'affiliation et ainsi obtenir un numéro ou code d'accréditation ainsi que mentionné précédemment dans la description.

Ce code d'accréditation lui permet de s'identifier à chaque connexion pour demande de validation d'une transaction, c'est à dire d'un paiement, et, le cas échéant, pour demande de mise en recouvrement de tout billet virtuel correspondant.

Sur la figure 3b, les références chiffrées désignent des opérations réalisées par les modules de numéros correspondants sur la figure 3a. A partir d'une étape DEBUT, 1a, correspondant à une position d'attente à une étape 1b du module de contrôle d'accès 1, le module de contrôle d'accès 1 précité communique le numéro d'accréditation et opère en une étape 1c une vérification du contrôle d'accès par lecture de la liste des vendeurs accrédités LVA mémorisés sur le module HDD1. Le module de contrôle d'accès 1 permet, bien sûr, de vérifier

l'adéquation entre le code d'accréditation présenté et l'adresse IP par exemple ainsi que les différents identificateurs du réseau Internet lorsque ce dernier est utilisé.

En cas de difficulté, il est possible de rendre ce numéro ou code d'accréditation variable et ainsi de fournir au vendeur accrédité une disquette contenant un programme non lisible permettant de fournir un code différent à chaque accès selon la date, l'heure ou tout autre paramètre. Le module de contrôle d'accès assure la vérification, la correspondance entre tous les paramètres du terminal vendeur TV.

Dans le cas où le code d'accréditation n'est pas valide à l'étape 1c, l'accès est refusé et le serveur est replacé en position de DEBUT 1a.

Si au contraire l'accès est accepté, le module de contrôle d'accès 1 procède à la communication des numéros uniques des billets électroniques au module 2 de vérification du numéro unique NU.

Le serveur dispose en fait de la liste exacte des billets électroniques valides et connaît, en conséquence, si un numéro unique est valide ou non. Cette opération réalisée à l'étape 2a sur la figure 3b peut correspondre à celle déjà mentionnée dans la description en liaison avec les figures 2d et 2f.

Si à l'étape 2a le numéro unique de billet électronique est valide, alors le module 2 transmet un ordre d'exécution au module 3 de notification de message de validation lequel à l'étape 3a envoie un message de validité de transaction par l'intermédiaire de la liaison du serveur au réseau étendu par exemple, le serveur

revenant en position de début afin de permettre, le cas échéant, de créditer le compte du vendeur et d'invalider le numéro unique correspondant pendant une durée de viduité, ainsi qu'il sera décrit ultérieurement dans la description. Si au contraire, le numéro unique à l'étape 2a n'est pas reconnu comme valide, le module 2 lance une commande au module 4 de comptage de comparaison du nombre d'erreurs, lequel, à l'opération 4a lors de la détection de trois erreurs successives par exemple, assure la déconnexion et l'invalidation de l'accréditation ainsi que, le cas échéant, la mise en mémoire des références du vendeur dans une liste de fraudeurs identifiés.

Dans un tel cas, le vendeur doit établir une connexion de rétablissement qui permet de bien contrôler que l'identité de ce demandeur n'a pas été usurpée par une personne non habilitée et que ces erreurs proviennent alors d'un client de ce vendeur, client identifié ou non.

Le vendeur doit alors se déconnecter de son client, l'identifier avant déconnexion et, bien entendu, communiquer cette identification au système serveur gestionnaire représenté en figure 3a.

La mise en œuvre de la procédure d'identification et de contrôle sur un nombre d'erreurs successives puis ré-accréditation du vendeur permet de supprimer tout risque de fraude sensible.

Un protocole spécifique de paiement d'achat de produits ou services par commerce électronique entre un terminal client TC, un terminal vendeur TV de produits ou services et, bien entendu, le serveur S gestionnaire de transactions réalisées au moyen de billets électroniques de valeur fiduciaire, conformes à l'objet de la présente

invention, sera maintenant décrit en liaison avec les figures 4a à 4b.

D'une manière générale, on indique que le terminal client TC est détenteur de billets électroniques de valeur fiduciaire tel que décrit précédemment dans la description.

Ces billets électroniques peuvent être distribués par un serveur spécifique ou, le cas échéant, par tout moyen ainsi qu'il sera décrit ultérieurement dans la description. Bien entendu, le serveur spécifique et les organes de distribution de ces billets électroniques sont contrôlés par l'entité d'émission. Des billets électroniques sont mémorisés dans le terminal client TC.

Le terminal vendeur TV est géré et contrôlé par un vendeur agréé, lequel s'est vu attribuer un numéro ou code d'accréditation permettant à ce dernier un accès au serveur gestionnaire, tel que décrit précédemment et dans les conditions décrites en liaison avec la figure 3a et la figure 3b.

On se trouve ainsi dans une situation de départ notée ST à la figure 4a mettant en relation le serveur S, le terminal client TC , le terminal vendeur TV.

Cette situation de départ ST correspond à celle dans laquelle, lors de la conduite d'un accord d'achat-vente de produits ou services pour un prix d'achat déterminé PA, le client a établi un ensemble de billets électroniques, chaque billet B_i ayant une valeur faciale ou contre-valeur monétaire CVMi, le client ayant choisi dans ses billets un ensemble de billets noté $[B_i]_{i=k}^{i=k+p}$ dont la somme de la valeur faciale couvre le prix d'achat PA.

Suite à l'accord d'achat-vente entre le terminal client et le terminal vendeur, le protocole de paiement, objet de l'invention, consiste au moins en une étape A à transmettre, à titre de paiement de transaction, du terminal client TC au terminal vendeur TV, un ensemble de billets électroniques, l'ensemble $[B_i]_{i=k}^{i=k+p}$ précité dont la somme de la valeur faciale couvre le prix d'achat PA.

Cette opération à l'étape A est notée transmission de :

$$[B_i]_{i=k}^{i=k+p} \Rightarrow \sum_{i=k}^{i=k+p} CVM_i = PA$$

L'étape A précitée est alors suivie d'une étape B consistant à transmettre, du terminal vendeur TV à l'organisme serveur spécifique S, l'ensemble de billets électroniques, support de la transaction pour authentification. Cette opération est réalisée à l'étape B par l'intermédiaire d'une sous étape B1 laquelle est suivie d'une sous étape B2 d'authentification du numéro unique NU_i* candidat au numéro unique NU_i de référence mémorisé au niveau du module HDD2, ainsi que mentionné en liaison avec la figure 3a. Cette opération est réalisée pour tous les billets B_i.

Sur procédure d'authentification réussie à la sous étape B2, cette procédure d'authentification étant représentée de manière simplifiée par la relation :

$$\forall_i NU_i^* = NU_i,$$

à chaque billet de l'ensemble de billets électroniques, support de la transaction étant reconnue la valeur faciale qui lui est dévolue, l'étape B est alors suivie d'une étape C consistant à transmettre de l'organisme serveur spécifique S au terminal vendeur TV un message de validation de paiement noté MVP_V.

L'étape C précitée est alors suivie avantageusement d'une étape D consistant à invalider au moins au niveau du serveur spécifique S tout billet électronique B_i de l'ensemble de billets électroniques, support de la transaction, pendant un délai de viduité spécifique. On comprend en particulier que l'invalidation des billets électroniques de l'ensemble de billets électroniques, support de la transaction, pendant ce délai de viduité, lequel peut être pris égal à un, deux ou trois ans, permet en fait de ne pas réutiliser le numéro unique attribué à chacun des billets pendant ce délai, afin de ne pas rediffuser les codes correspondants des numéros uniques pendant le délai de viduité précité. Ceci permet de réduire la vulnérabilité des billets électroniques, objets de la présente invention, aux attaques des fraudeurs intempestifs sur le réseau.

Sur réponse négative aux tests à la sous étape B2, l'authentification du numéro unique n'étant pas réussie, le protocole de paiement, objet de l'invention consiste à une étape J à transmettre, de l'organisme serveur spécifique S au terminal vendeur TV, un message noté MIVP d'invalidation de paiement et de non validation de la transaction.

La figure 4b représente une variante de mise en œuvre du protocole, objet de la présente invention tel que représenté en figure 4a.

Dans la variante précitée, suite à l'étape A consistant à transmettre à titre de paiement de transaction un ensemble de billets électroniques, support de la transaction, l'ensemble $[B_i]_{i=k}^{i=k+p}$, cette étape étant représentée à l'étape effective A1 de la figure 4b, le protocole objet de l'invention dans ce mode de réalisation consiste, en une sous étape A2, à inhiber, au moins temporairement au niveau du terminal client TC, l'utilisation par ce terminal client de tout billet électronique appartenant à l'ensemble de billets électroniques support de cette transaction.

Cette inhibition temporaire peut être maintenue avantageusement au moins jusqu'à l'invalidation, au moins au niveau du serveur spécifique S de tout billet électronique de cet ensemble de billets électroniques pendant le délai de viduité sur procédure d'authentification réussie.

On comprend en particulier que la sous-étape d'inhibition temporaire A2 permet ainsi de supprimer tout risque d'utilisation multiple successive de billets électroniques comportant un même numéro unique pour des transactions distinctes, que cette utilisation successive soit frauduleuse de la part de l'utilisateur du terminal client TC ou fortuite. Cette inhibition temporaire peut alors permettre de renforcer la sécurité des tiers dans la conduite des transactions vis-à-vis d'une transaction déjà réalisée par le terminal client TC.

A titre d'exemple non limitatif, on indique que l'opération réalisée à la sous-étape A2 d'inhibition temporaire peut consister dans le terminal client TC à provoquer la mémorisation de tout billet électronique utilisé pour une transaction spécifique dans une liste ou dans un fichier archivé et dont l'accès en lecture est rendu conditionnel à une autorisation du serveur par l'intermédiaire du terminal vendeur par exemple, ainsi qu'il sera décrit ultérieurement dans la description.

En outre, ainsi que représenté également en figure 4, le protocole, objet de la présente invention, peut consister suite à l'étape C consistant à transmettre de l'organisme serveur spécifique S au terminal vendeur agréé TV un message de validation de paiement, à réaliser en outre une opération E de transmission du terminal vendeur agréé TV au terminal client TC un message d'accusé de réception de paiement de transaction, puis, sur réception du message d'accusé de réception de paiement par le terminal client TC, à effacer dans le terminal client TC chaque billet électronique de l'ensemble de billets électroniques noté $[B_i]_{i=k}^{i=k+p}$, objet ou support de la transaction.

On comprend en particulier que l'étape F d'effacement précité peut être réalisée sur la liste de billets électroniques soumis à inhibition temporaire et mémorisés dans un fichier spécifique tel que mentionné précédemment dans la description.

Enfin, ainsi que représenté en figure 4a, le protocole, objet de la présente invention, peut consister, suite à l'étape C, transmission de l'organe serveur spécifique S au terminal vendeur TV d'un message de

validation de paiement, à réaliser, en outre, à l'initiative du vendeur agréé, utilisateur du terminal vendeur, une étape G consistant à transmettre du terminal vendeur à l'organisme serveur spécifique S une requête d'accréditation de compte bancaire notée REQ_AC_CB, compte bancaire au nom du vendeur agréé pour un montant correspondant du montant de la transaction. Sur la figure 4a, en raison de la réalisation de l'étape G conditionnelle à l'initiative du vendeur, le lien entre l'étape C et l'étape G est représentée en traits mixtes.

Sur acceptation de la requête d'accréditation REQ_AC_CB, l'étape G est alors suivie d'une étape H de renvoi d'un accusé de réception et de validation de la requête au terminal vendeur agréé TV, l'accusé de réception étant noté MACK_V.

L'étape H est alors suivie d'une étape I consistant à effacer, au niveau du terminal vendeur agréé TV, tout billet électronique de cet ensemble de billets électroniques, l'ensemble $[B_i]_{i=k}^{i=k+p}$, support de la transaction, et ayant fait l'objet d'une mise en recouvrement.

Un mode de mise en œuvre spécifique non limitatif de l'attribution de délai de viduité à l'un des billets électroniques par l'organisme serveur spécifique S conformément au protocole de paiement, objet de la présente invention, sera maintenant décrit en liaison avec la figure 4d.

Ce mode de gestion spécifique prend en compte une situation de départ ST dans laquelle le serveur S s'est vu notifier l'ensemble des billets électroniques, support

d'une transaction, l'ensemble $[B_i]_{i=k}^{i=k+p}$, et où un message de validation de paiement MVP_V a été transmis à l'étape C vers le terminal vendeur TV.

En conséquence, la figure 4d représente un mode de mise en œuvre non limitatif de l'étape D de la figure 4a.

Ce mode de mise en œuvre prend en compte l'existence ou la non-existence d'une requête d'accréditation de compte bancaire à l'initiative du terminal vendeur à l'étape G.

Dans ce but, le serveur S réalise une étape de vérification D1 consistant à vérifier l'existence d'une requête d'accréditation REQ_AC_CB du compte bancaire à l'initiative du vendeur. Sur réponse positive à l'étape de vérification D1, une étape D4 est réalisée par le serveur consistant à effectuer une invalidation interne et externe de tout ensemble de billets, support d'une transaction, l'ensemble $[B_i]_{i=k}^{i=k+p}$, l'invalidation interne consistant dans le serveur à attribuer un délai de viduité DV_i à chaque billet B_i très supérieur à la durée de validité $DVID_i$ de chacun des billets B_i correspondant. La durée de viduité $DVID_i$ peut correspondre à la durée de deux ou trois ans mentionnée précédemment dans la description.

En ce qui concerne l'invalidation externe de chacun des billets B_i précités, on indique que cette invalidation est effectuée suite à l'étape C et parallèlement à l'invalidation interne réalisée à l'étape B, et en particulier à la sous-étape D4 précitée par l'intermédiaire des étapes E et F dans le terminal client, ainsi bien entendu qu'à l'étape I dans le terminal

vendeur TC, ainsi que décrit précédemment dans la description en liaison avec la figure 4a.

Au contraire, sur réponse négative à l'étape de vérification D1, une étape D2 d'invalidation interne seule de l'ensemble des billets électroniques, support de la transaction l'ensemble $[B_i]_{i=k}^{i=k+p}$ est effectuée dans le serveur S, cette étape D2 pouvant consister dans le serveur à mémoriser la liste des billets constitutifs de cet ensemble de billets dans un répertoire spécifique auquel est allouée une durée de viduité $DVID_i$ correspondant à la durée de validité de chacun des billets $DVID_i$ au maximum.

L'opération réalisée à la sous étape B2 permet alors au serveur, en l'absence de requête d'accréditation de compte bancaire au nom du vendeur, d'assurer l'échange de billets électroniques entre différents vendeurs ou, le cas échéant, entre vendeurs et tiers pendant la durée de validité DV_i allouée à chaque billet B_i. On comprend bien sûr que cette étape d'échange peut être réalisée indépendamment du serveur S pendant la durée de validité précitée à l'étape D3, chaque possesseur d'un billet dont la durée de validité est alors affichée pouvant continuer l'échange pendant cette durée de validité ou, le cas échéant, procéder à une demande d'accréditation de compte bancaire selon les étapes G, H, I décrites précédemment en figure 4a.

Pour réaliser une telle demande d'accréditation, le tiers non identifié peut se déclarer auprès du serveur ou de tout serveur habilité à réaliser une accréditation de compte bancaire au nom de l'utilisateur tiers.

Une description plus détaillée d'un mode de réalisation préférentiel non limitatif du protocole de paiement d'achat de produits ou services par commerce électronique, objet de la présente invention, sera maintenant donnée en liaison avec la figure 5.

Le mode de réalisation précité permet, pour une somme de la valeur faciale transmise supérieure au prix d'achat PA, somme visant à effectuer le règlement du prix d'achat, d'introduire une procédure de rendu de monnaie en unité monétaire de compte.

L'introduction d'une telle procédure apparaît particulièrement remarquable en raison du fait que celle-ci permet alors de rapprocher de manière quasi parfaite le protocole de paiement, objet de la présente invention, dans le cadre du commerce électronique, de celui d'un paiement classique par échange de papier monnaie entre le vendeur et l'acheteur.

En référence à la figure 5 précitée, la procédure de rendu de monnaie peut être mise en œuvre après l'étape A de la figure 4a.

Dans ces conditions, ainsi que représenté à la figure 5, le protocole objet de la présente invention consiste au moins, en une étape B'1), à transmettre, du terminal vendeur TV à l'organisme serveur spécifique S, l'ensemble $[B_i]_{i=k}^{i=k+p}$ des billets virtuels, support de la transaction, ainsi que, bien entendu, la valeur du prix d'achat PA pour authentification. L'étape B'1 précitée est alors suivie de l'étape d'authentification B'2, laquelle peut être identique à l'étape B2 de la figure 4, pour constituer l'étape B' semblable à l'étape B de la figure 4a précitée. En outre, et de manière non limitative, on

indique que l'étape B'2 d'authentification peut comporter, outre la vérification de l'égalité des champs candidats NU_i* et des champs d'origine NU_i pour chacun des billets d'indice i, la vérification de la supériorité de la somme de la valeur faciale de l'ensemble des billets transmis B_i, support de la transaction au prix d'achat PA.

L'étape B', sur procédure d'authentification réussie et à chaque billet de l'ensemble de billets électroniques, support de la transaction, étant reconnue la valeur faciale qui lui est dévolue, est suivie d'une étape C' consistant à transmettre, du système organisme serveur spécifique S au terminal vendeur TV, le message de validation de paiement MVP_V ainsi qu'un sous ensemble de billets électroniques, ensemble noté $[SB_i]_{i=m}^{i=m+n}$, dont la somme de la valeur faciale couvre la différence entre la somme de valeur faciale transmise et le prix PA. On comprend, bien entendu, que chaque billet du sous ensemble de billets électroniques est établi dans la même unité monétaire de compte que celle des billets de l'ensemble de billets électroniques transmis, support de la transaction et que, de cette manière, la monnaie peut être rendue en unité monétaire de compte correspondante. La notion de sous ensemble de billets électroniques dont la somme de la valeur faciale couvre la différence entre la somme de valeur faciale transmise et le prix d'achat désigne tout sous ensemble de billets électroniques de la classe des billets électroniques définis précédemment dans la description pour les billets de valeur faciale différente précédemment décrits.

L'étape C' est alors suivie d'une étape E'1 consistant à transmettre, du terminal vendeur TV au

terminal client TC, le sous ensemble de billets électroniques au titre de monnaie rendue et noté $[SB_i]_{i=m}^{i=m+n}$.

On indique de manière non limitative que la transmission du terminal vendeur TV au terminal client TC du sous-ensemble de billets électroniques au titre de monnaie rendue $[SB_i]_{i=m}^{i=m+n}$ peut être effectuée, ainsi que représenté sur la figure 5, simultanément à la transmission du message MVPT_C de validation de paiement. De préférence, à chaque billet du sous-ensemble de billets de monnaie rendue peut également être affectée, au titre de variable auxiliaire, l'adresse du terminal client TC de manière analogue au mode de réalisation déjà décrit précédemment dans la description pour la transaction terminal client, terminal vendeur.

En outre, ainsi que représenté en figure 5, l'étape consistant à transmettre du terminal vendeur TV au terminal client TC le sous-ensemble de billets électroniques au titre de monnaie rendue, représentée à l'étape E'1 de la figure 5, peut être suivie d'une étape d'effacement, notée E'2, dans le terminal vendeur TV de chaque billet électronique du sous-ensemble de billets électroniques au titre de monnaie rendue $[SB_i]_{i=m}^{i=m+n}$. Sur la figure 5, de manière non limitative, les étapes E'1 et E'2 sont réputées définir une étape E', laquelle apparaît comme une étape perfectionnée par rapport à l'étape E de la figure 4a. L'étape E' est alors suivie de l'étape F de la figure 4a consistant en un effacement de l'ensemble des

billets électroniques, support de la transaction $[B_i]_{i=k}^{i=k+p}$ dans le terminal client TC.

Différentes indications seront maintenant données en ce qui concerne le mode d'acquisition par un client quelconque muni d'un terminal client TC de billets électroniques permettant à ce dernier de mettre en œuvre le protocole, objet de la présente invention.

En ce qui concerne l'acquisition de billets virtuels, cette acquisition par le client précité peut être réalisée par exemple de trois manières différentes :

- dans un commerce quelconque, les billets virtuels pouvant se présenter sous forme de cartes plastifiées comportant au moins un enregistrement d'un ou plusieurs billets virtuels. De préférence, la zone d'enregistrement des billets virtuels précités peut être constituée par une zone effaçable, laquelle permet au client considéré d'introduire par exemple les billets virtuels dans son terminal client TC, la première introduction assurant l'effacement de la zone d'enregistrement précitée sur la carte plastifiée par exemple.
- Le client précité peut également acheter des billets virtuels de valeur fiduciaire conformes à l'objet de la présente invention dans un guichet distributeur automatique de billets, désigné guichet DAB.

  Dans ces conditions, le client introduit par exemple une carte bancaire, de type carte à puce, dans la fente du guichet DAB, choisit l'achat de billets électroniques de valeur fiduciaire. Le guichet DAB se connecte au serveur spécifique et réalise l'opération de demande de transfert de billets virtuels vers la

carte bancaire du client. Lorsque les billets virtuels sont acquis par ce dernier, un débit automatique du compte de la carte bancaire de la somme correspondante est effectué et un ticket ou facturette correspondant à la transaction est délivré(e) au client. On comprend en particulier que l'édition de ce ticket revient à l'impression du reçu du retrait actuel délivré lors de transactions à partir de cartes bancaires. Bien entendu, et comme dans le cas du papier monnaie, le client, acheteur des billets virtuels, possesseur de ces billets, est responsable, non seulement de l'utilisation de ces billets virtuels, mais également de leur reproduction et de toute contribution à la reproduction de ces billets, de la même manière que dans le cas de billets en papier.

- Le client peut également acheter des billets sur Internet par connexion au site serveur spécifique S, la transaction pouvant également être réalisée à partir d'un terminal lecteur de carte bancaire par exemple. Les billets virtuels sont alors directement téléchargés sur son terminal client TC, un programme de gestion spécifique pouvant être implanté sur le terminal client TC précité.

Les billets virtuels et le protocole de paiement d'achat, objets de la présente invention, permettent, contrairement au système de paiement électronique actuel par carte bancaire, de réaliser des paiements d'achats très proches de la réalisation de paiements d'achats à partir de papier monnaie pour les raisons ci-après :

- en premier lieu, le possesseur de billets virtuels est possesseur de ces billets dans les mêmes conditions que le possesseur de billets en papier monnaie ;
- l'échange de billets virtuels entre utilisateurs est réalisé de manière semblable à l'échange de billets en papier monnaie, tout échange étant réalisé de manière totalement anonyme pour le client et pour tout client successif, seul le destinataire c'est-à-dire le vendeur pouvant, le cas échéant, apparaître comme titulaire des billets qu'il possède, ce qui bien entendu n'ajoute aucune information sur la transaction réalisée ;
- la perte ou la substitution, frauduleuse ou non, d'un billet électronique de valeur fiduciaire a pour conséquence la perte ou la substitution de la valeur faciale en unité monétaire de compte correspondante comme dans le cas d'un billet en papier monnaie ;
- la sécurisation des billets électroniques virtuels peut être rendue supérieure à celle des billets en papier monnaie en raison, d'une part, de l'existence d'un codage spécifique entre le numéro unique représentatif d'une contre valeur monétaire particulière, et, d'autre part, de la protection d'un tel codage par un procédé de chiffrement, ce qui bien entendu rend d'autant plus délicat toute tentative de percement et de reproduction de l'ensemble ; toute tentative apparaît d'autant plus illusoire que les moyens informatiques nécessaires à leur mise en œuvre représentent un investissement sans commune mesure avec la valeur du billet virtuel, objet de l'attaque.

REVENDICATIONS

1. Billet électronique de valeur fiduciaire, caractérisé en ce qu'il comprend au moins un champ représentatif d'un numéro unique représentatif d'une contre-valeur monétaire, établie dans une unité monétaire de compte, par une entité d'émission, ledit numéro unique codé selon une combinaison de caractères en fonction de la contre-valeur monétaire présentant une probabilité de découverte de ladite combinaison liée à cette contre-valeur monétaire.

2. Billet selon la revendication 1, caractérisé en ce que le champ représentatif d'un numéro unique est constitué par un ensemble de caractères alphanumériques, le nombre de caractères alphanumériques de cet ensemble de caractères alphanumériques étant fonction de ladite contre-valeur monétaire attribuée audit numéro unique.

3. Billet selon la revendication 2, caractérisé en ce que ledit ensemble de caractères alphanumériques comporte au moins :

- un nombre déterminé de digits fonction de ladite contre-valeur monétaire attribuée audit numéro unique, lesdits digits étant représentatifs d'un nombre unique lié à ladite contre-valeur monétaire ;
- un nombre déterminé de caractères alphanumériques, inférieur au nombre de digits, au moins un caractère alphanumérique étant inséré entre deux digits.

4. Billet selon la revendication 3, caractérisé en ce que lesdits caractères alphanumériques sont insérés à des emplacements de position aléatoire entre deux digits successifs.

5. Billet selon l'une des revendications précédentes, caractérisé en ce que celui-ci comprend en outre un champ auxiliaire représentatif de l'entité d'émission et du pays hôte de cette entité d'émission.

6. Billet selon l'une des revendications précédentes, caractérisé en ce que celui-ci comprend en outre un champ auxiliaire représentatif de la durée de validité dudit billet.

7. Billet selon l'une des revendications précédentes, caractérisé en ce que ledit billet comprend en outre un champ auxiliaire représentatif de la valeur faciale dudit billet.

8. Billet selon l'une des revendications précédentes, caractérisé en ce que le champ représentatif dudit numéro unique est constitué par une valeur chiffrée à partir d'une pluralité de variables comprenant au moins ledit numéro unique, l'entité d'émission, la valeur faciale et l'unité monétaire de compte, ce qui permet, à partir d'une opération de déchiffrement, d'effectuer toute opération d'authentification et de non répudiation dudit billet par ladite entité d'émission.

9. Billet selon l'une des revendications 1 à 8, caractérisé en ce que ladite valeur faciale du billet est une valeur dédiée, établie à la demande d'un utilisateur par ladite entité d'émission.

10. Billet selon l'une des revendications 8 ou 9, caractérisé en ce que ladite pluralité de variables comprend en outre l'adresse électronique du terminal créancier, destinataire de ce billet électronique en exécution d'une transaction, ce qui permet, d'une part, de justifier de la possession dudit billet par ce terminal

créancier et ce destinataire suite à une validation de cette transaction, et, d'autre part, d'assurer un échange sécurisé d'un même billet électronique au cours de transactions successives par simple remplacement dans ladite pluralité de variables de l'adresse électronique du terminal créancier destinataire de ce billet électronique.

11. Système serveur gestionnaire de transactions réalisées au moyen de billets électroniques de valeur fiduciaire selon les revendications 1 à 10, entre un acheteur et un vendeur, caractérisé en ce qu'il comporte au moins :

- des moyens de mémorisation d'un ensemble de vendeurs accrédités, habilités à conclure une ou plusieurs transactions au moyen desdits billets électroniques de valeur fiduciaire ;
- des moyens de mémorisation de listes de billets électroniques de valeur fiduciaire émis valides, respectivement invalides, pendant une durée de viduité ;
- des moyens de contrôle et d'authentification d'accès audit système serveur de tout vendeur accrédité en vue d'une opération de mise en recouvrement de billets électroniques de valeur fiduciaire échangés au cours d'au moins une transaction ;
- des moyens de vérification de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé à partir d'au moins une liste des billets électroniques de valeur fiduciaire électroniques émis valides ;
- des moyens de notification audit vendeur accrédité d'un message de validation de transaction entre ledit

vendeur et un acheteur quelconque, permettant l'envoi audit vendeur d'un message de validation de transaction sur vérification positive de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé.

12. Système selon la revendication 11, caractérisé en ce que celui-ci comporte en outre :

- des moyens de comptage du nombre d'erreurs de vérification de la validité du numéro unique de chaque billet électronique de valeur fiduciaire échangé ;
- des moyens de comparaison du nombre d'erreurs de vérification de la validité dudit numéro unique à une valeur de seuil, lesdits moyens de comparaison pilotant lesdits moyens de notification et permettant l'envoi d'un message d'invalidation de transaction audit vendeur accrédité lorsque ce nombre d'erreurs de vérification est supérieur ou égal à ladite valeur de seuil.

13. Protocole de paiement d'achats de produits ou de services par commerce électronique entre un terminal client et un terminal vendeur de produits ou services, le terminal client étant détenteur de billets électroniques de valeur fiduciaire selon l'une des revendications 1 à 10, distribués par un organisme serveur spécifique, entité d'émission, et mémorisés dans ce terminal client, le terminal vendeur étant géré et contrôlé par un vendeur agréé auprès dudit organisme serveur spécifique, caractérisé en ce que, lors de la conduite d'un accord d'achat/vente de produits ou services pour un prix déterminé, ce protocole consiste au moins :

a) à transmettre à titre de paiement de transaction du terminal client au terminal vendeur un ensemble de billets électroniques dont la somme de la valeur faciale couvre le prix d'achat déterminé ;

b) à transmettre dudit terminal vendeur audit organisme serveur spécifique ledit ensemble de billets électroniques support de ladite transaction pour authentification par vérification de la validité du numéro unique de ces billets électroniques, et, sur procédure d'authentification réussie, à chaque billet électronique de cet ensemble de billets électroniques support de ladite transaction étant reconnue la valeur faciale qui lui est dévolue,

c) à transmettre dudit organisme serveur spécifique audit terminal vendeur un message de validation de paiement,

d) à invalider au moins, au niveau dudit organisme serveur spécifique, tout billet électronique de cet ensemble de billets électroniques support de cette transaction pendant un délai de viduité, et, sur procédure d'authentification non réussie,

e) à transmettre dudit organisme serveur spécifique audit terminal vendeur un message d'invalidation de paiement et de non validation de la transaction.

14. Protocole selon la revendication 13, caractérisé en ce que, suite à l'étape a) consistant à transmettre à titre de paiement de transaction un ensemble de billets électroniques support de la transaction, celui-ci consiste à inhiber, au moins temporairement, au niveau dudit terminal client, l'utilisation par ce terminal client de tout billet électronique appartenant à cet ensemble de billets électroniques support de cette

transaction, ladite inhibition temporaire étant maintenue au moins jusqu'à l'invalidation, au moins au niveau dudit serveur spécifique, de tout billet électronique de cet ensemble de billets électroniques pendant le délai de viduité sur procédure d'authentification réussie.

15. Protocole selon les revendications 13 et 14, caractérisé en ce que, suite à l'étape c) consistant à transmettre dudit organisme serveur spécifique audit terminal vendeur agréé un message de validation de paiement, celui-ci consiste en outre :

- à transmettre dudit terminal vendeur agréé audit terminal client un message d'accusé de réception de paiement de transaction, et, sur réception dudit message d'accusé de réception de paiement par ledit terminal client,
- à effacer dans ledit terminal client chaque billet électronique de cet ensemble de billets électroniques objet de ladite transaction.

16. Protocole selon l'une des revendications 13 à 15, caractérisé en ce que, suite à l'étape c) consistant à transmettre dudit organisme serveur spécifique audit terminal vendeur un message de validation de paiement, celui-ci consiste en outre, à l'initiative du vendeur agréé utilisateur dudit terminal vendeur :

- à transmettre dudit terminal vendeur audit organisme serveur spécifique une requête d'accréditation de compte bancaire au nom dudit vendeur agréé pour un montant correspondant au paiement de ladite transaction, et, sur acceptation de ladite requête et renvoi d'un accusé de réception et de validation de ladite requête audit terminal vendeur agréé,

- à effacer, au niveau du terminal vendeur agréé, tout billet électronique de cet ensemble de billets électroniques objet de la transaction ayant fait l'objet d'une mise en recouvrement.

17. Protocole selon l'une des revendications 13 à 16, caractérisé en ce que, pour une somme de la valeur faciale transmise supérieure audit prix d'achat, celui-ci comprend en outre une procédure de rendu de monnaie en unité monétaire de compte.

18. Protocole selon la revendication 17, caractérisé en ce que, suite à l'étape a) de transmission à titre de paiement de transaction de ladite somme de valeur faciale transmise, ladite procédure de rendu de monnaie consiste au moins :

b') à transmettre dudit terminal vendeur audit organisme serveur spécifique ledit ensemble de billets électroniques support de ladite transaction et ledit prix d'achat pour authentification, et, sur procédure d'authentification réussie, à chaque billet électronique de cet ensemble de billets électroniques support de ladite transaction étant reconnue la valeur faciale qui lui est dévolue ;

c') à transmettre dudit organisme serveur spécifique audit terminal vendeur un message de validation de paiement et un sous-ensemble de billets électroniques dont la somme de la valeur faciale couvre la différence entre ladite somme de valeur faciale transmise et ledit prix d'achat, et

e'1) à transmettre dudit terminal vendeur audit terminal client ledit sous ensemble de billets électroniques au titre de monnaie rendue.

19. Protocole selon la revendication 18, caractérisé en ce que à l'étape consistant à transmettre dudit terminal vendeur au terminal client ledit sous ensemble de billets électroniques au titre de monnaie rendue est associée une étape d'effacement, dans ledit terminal vendeur, de chaque billet électronique dudit sous ensemble de billets électroniques au titre de monnaie rendue.

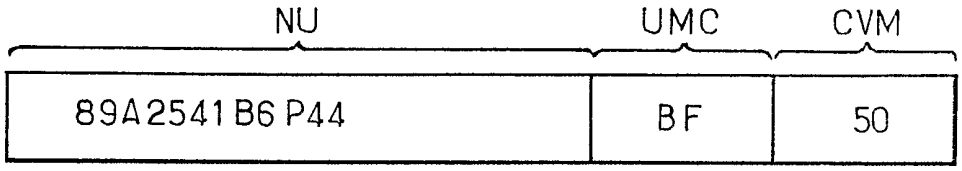


FIG.1a.

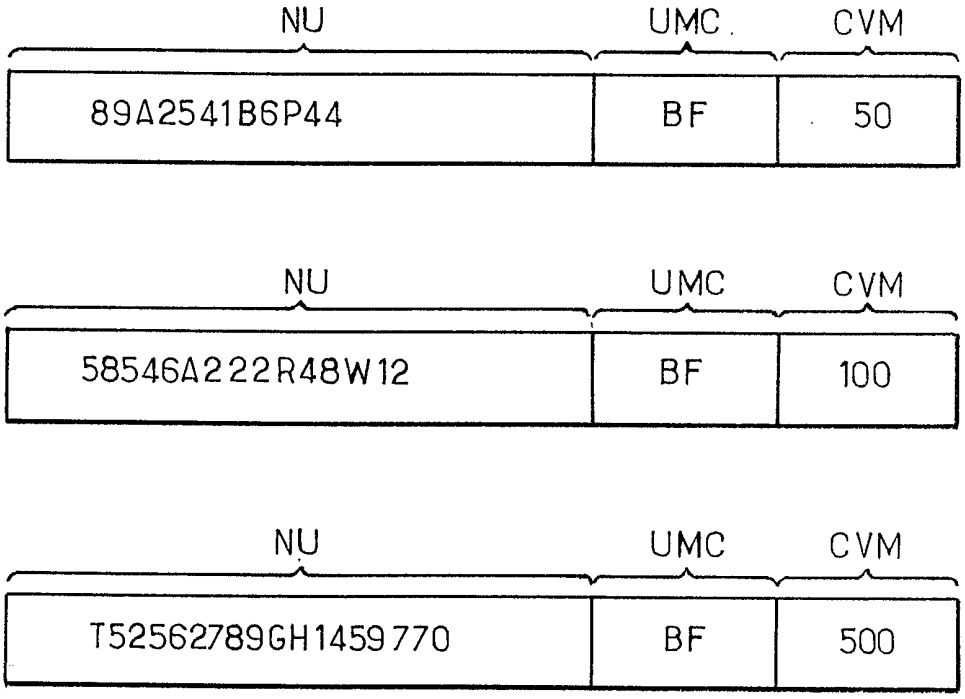


FIG.1b.

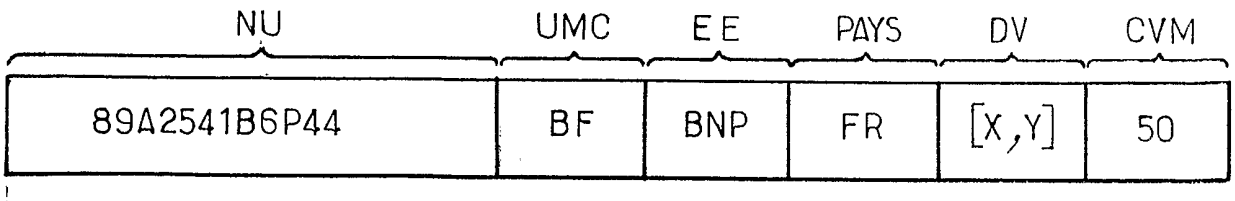


FIG.1c.

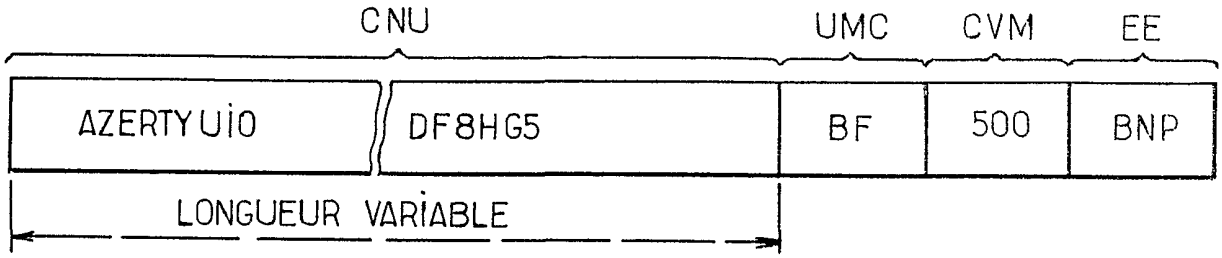


FIG.2a.

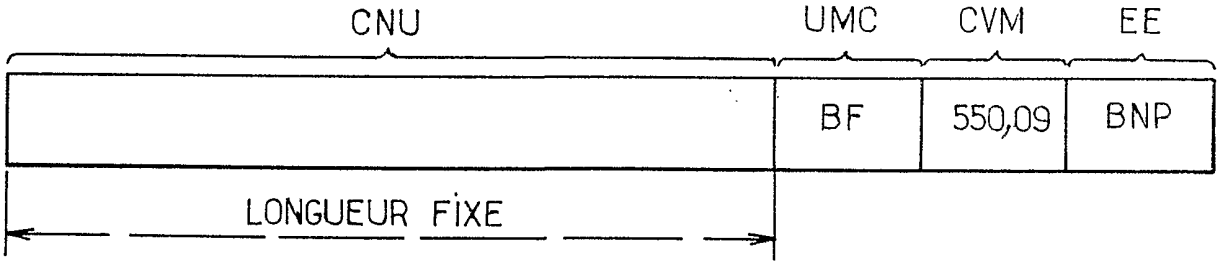


FIG.2b.

$\mathcal{C} = CNU = C_{KS}$ (NU, EE, CVM, UMC, ATV)

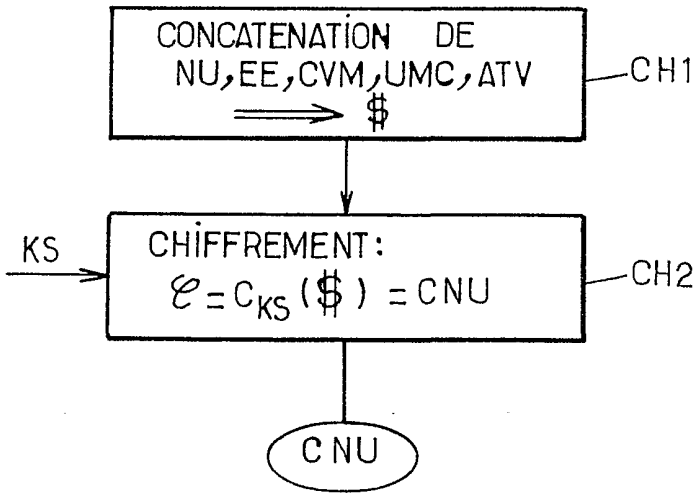


FIG.2c. CHIFFREMENT À PARTIR D'UNE CLÉ SECRÈTE KS

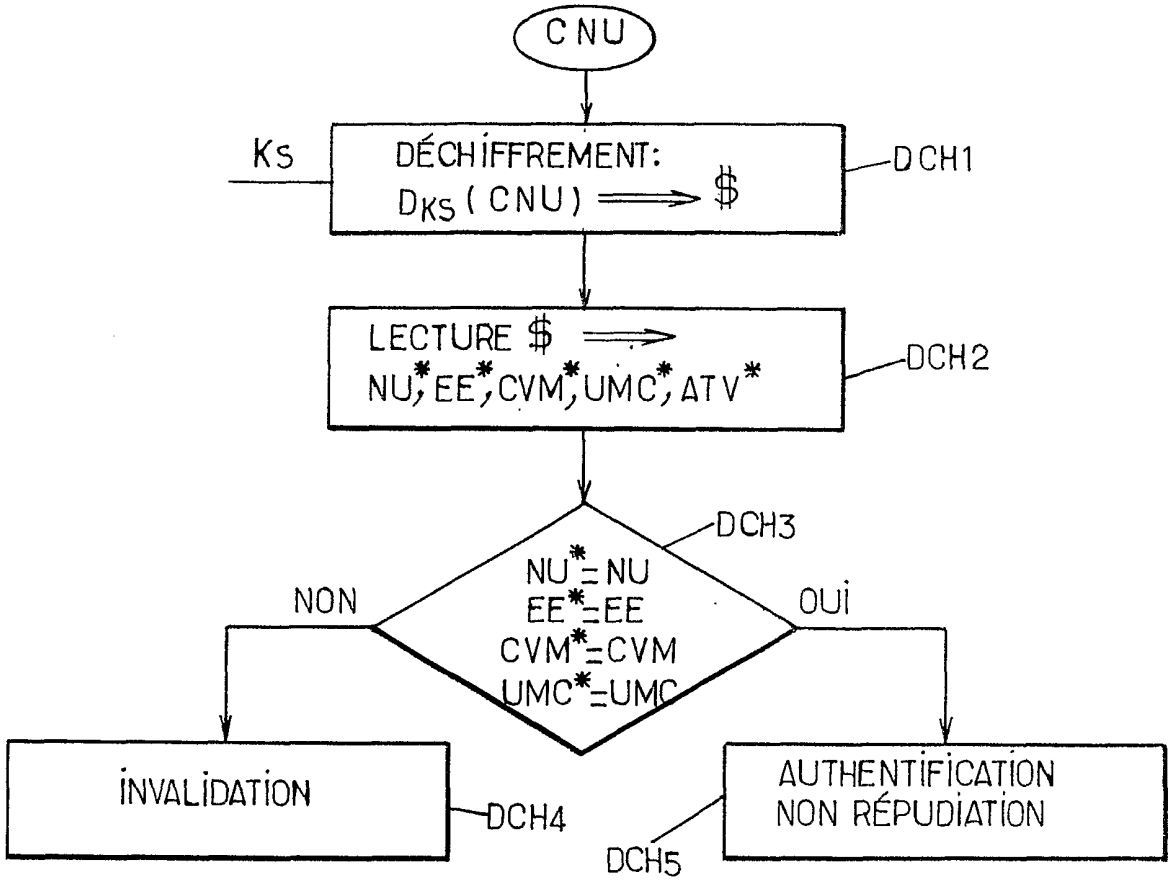


FIG.2d. DÉCHIFFREMENT À PARTIR DE LA CLÉ SECRÈTE Ks

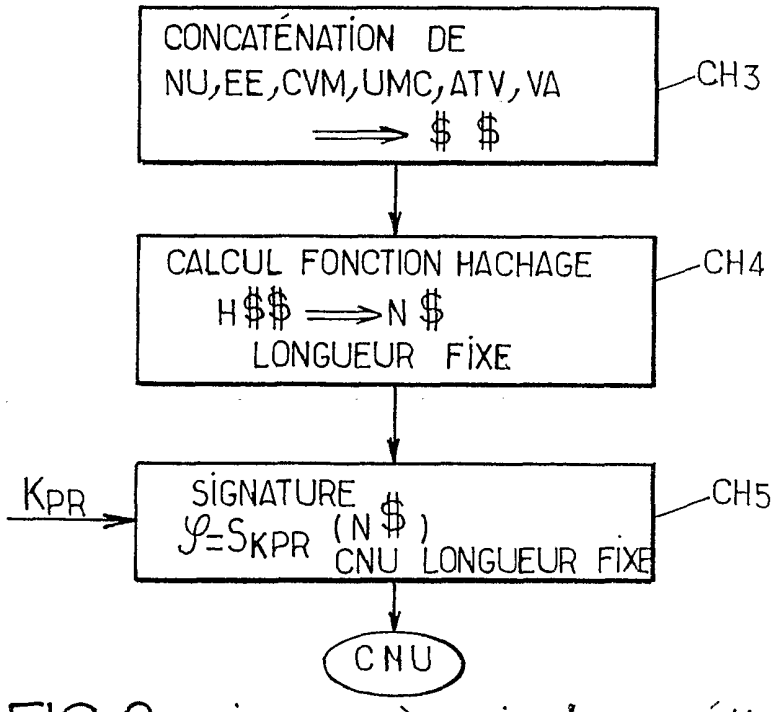


FIG.2e. SIGNATURE À PARTIR D'UNE CLÉ KPR

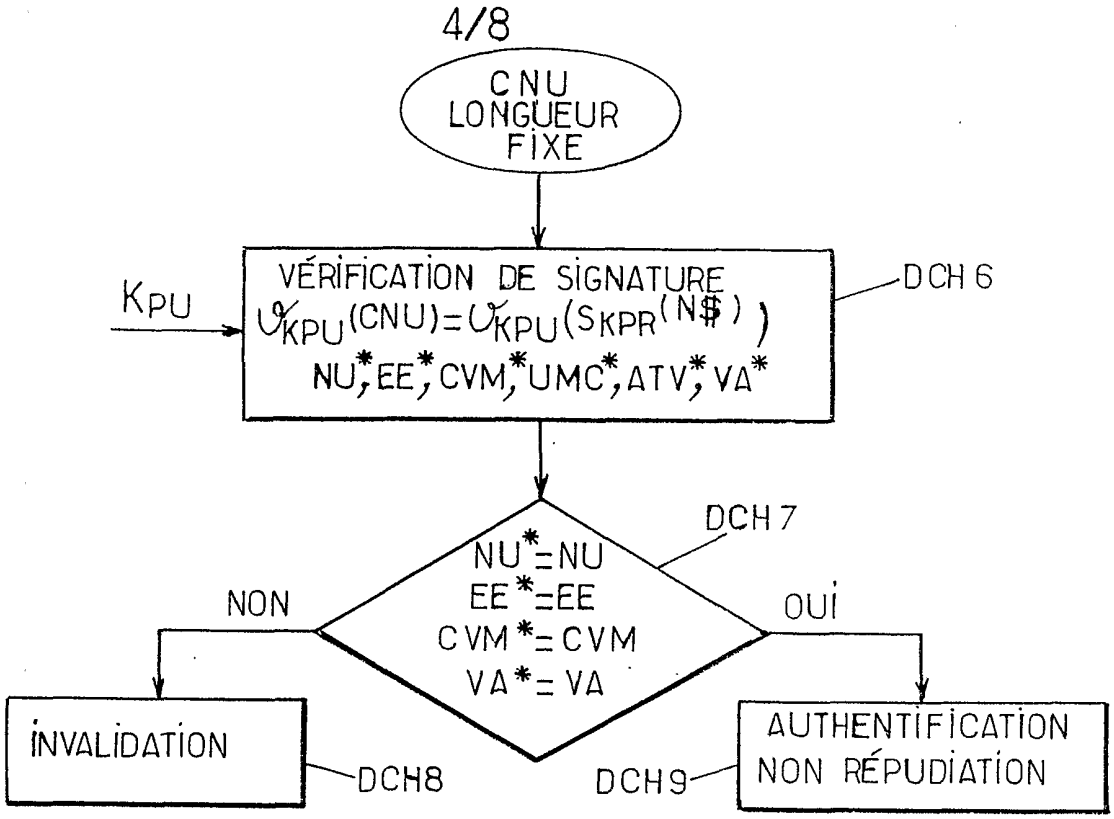


FIG.2f. VÉRIFICATION DE SIGNATURE A PARTIR D'UNE CLÉ DISSYMÉTRIQUE

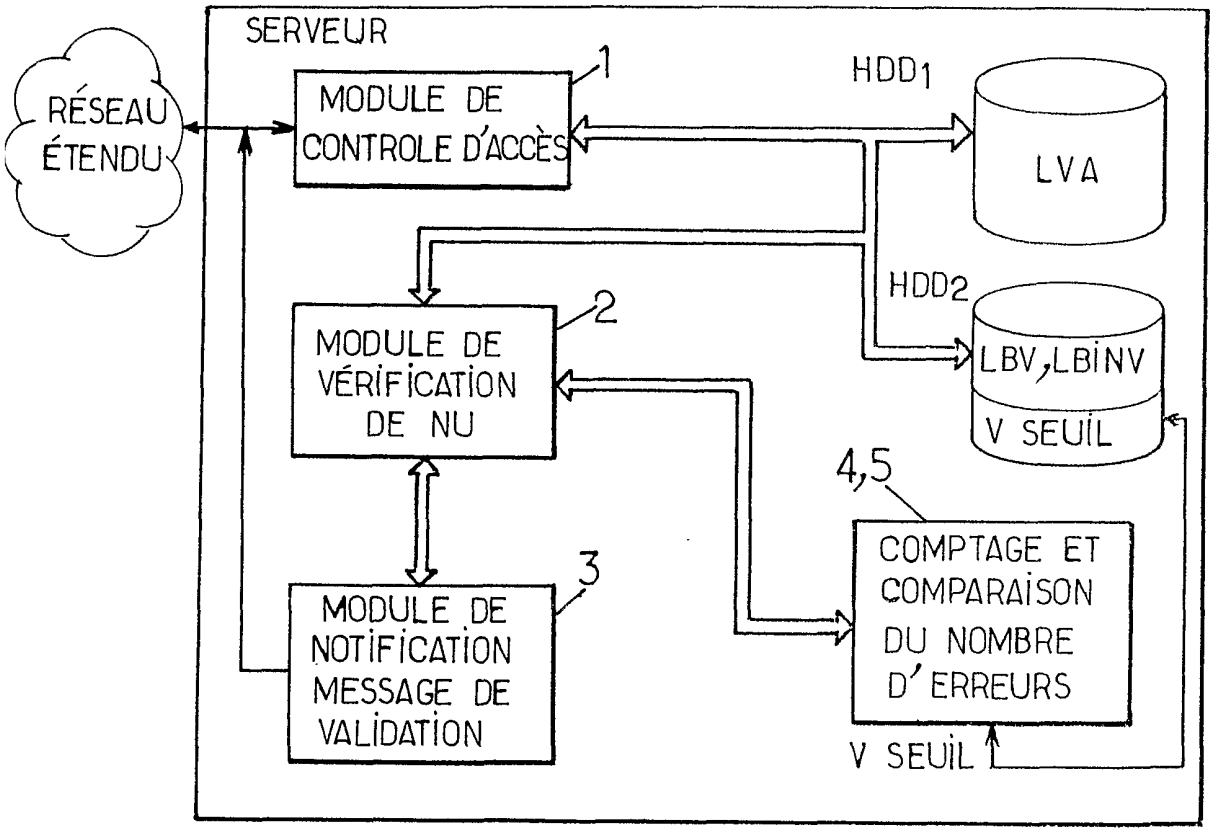


FIG.3a.

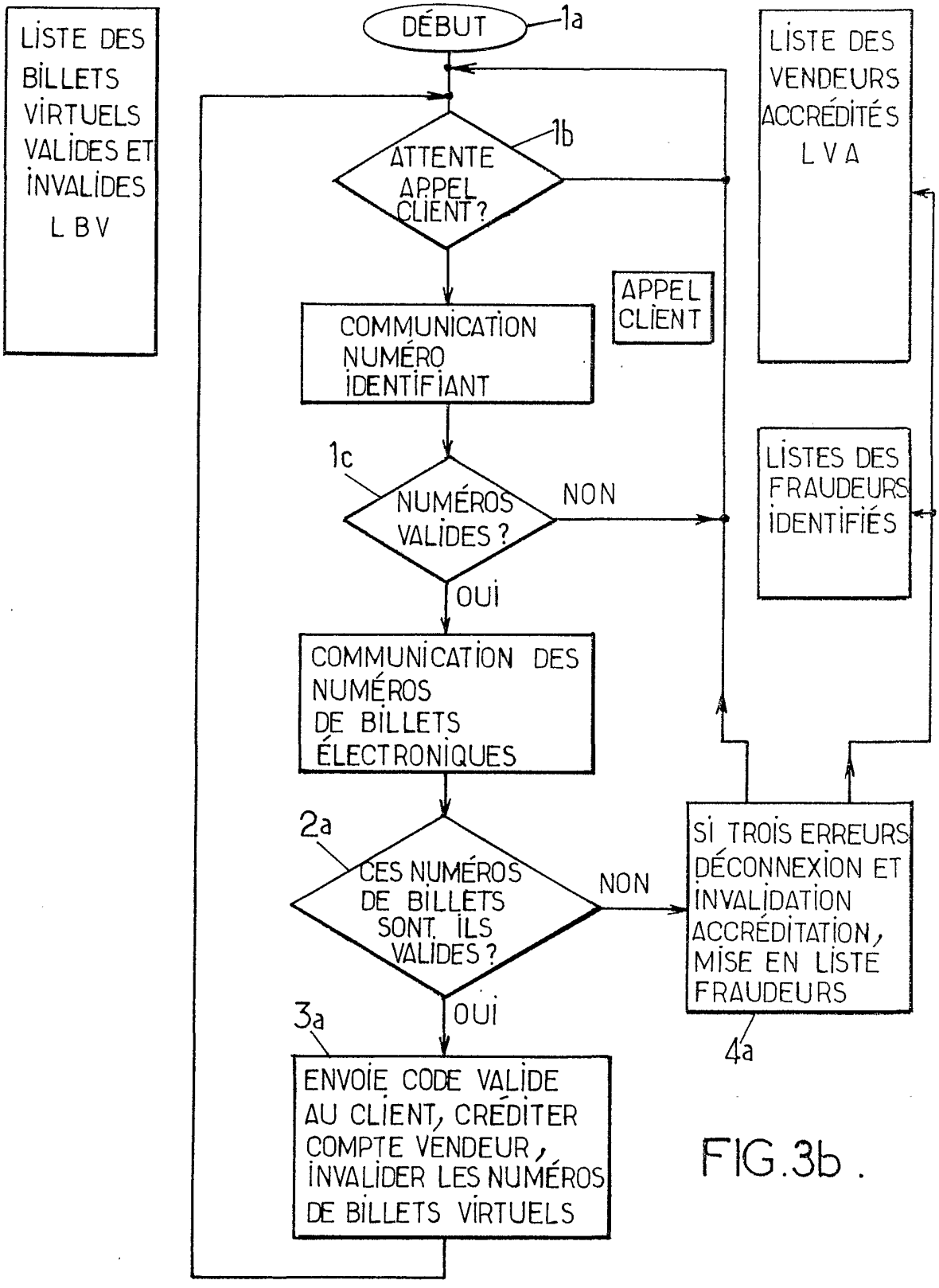

LISTE DES BILLETS VIRTUELS VALIDES ET INVALIDES L B V
DÉBUT
1a
ATTENTE APPEL CLIENT ?
1b
APPEL CLIENT
COMMUNICATION NUMÉRO IDENTIFIANT
1c
NUMÉROS VALIDES ?
NON
OUI
COMMUNICATION DES NUMÉROS DE BILLETS ÉLECTRONIQUES
2a
CES NUMÉROS DE BILLETS SONT ILS VALIDES ?
NON
OUI
3a
ENVOIE CODE VALIDE AU CLIENT, CRÉDITER COMPTE VENDEUR, INVALIDER LES NUMÉROS DE BILLETS VIRTUELS
SI TROIS ERREURS DÉCONNEXION ET INVALIDATION ACCRÉDITATION, MISE EN LISTE FRAUDEURS
4a
LISTE DES VENDEURS ACCRÉDITÉS L V A
LISTES DES FRAUDEURS IDENTIFIÉS

FIG.3b.

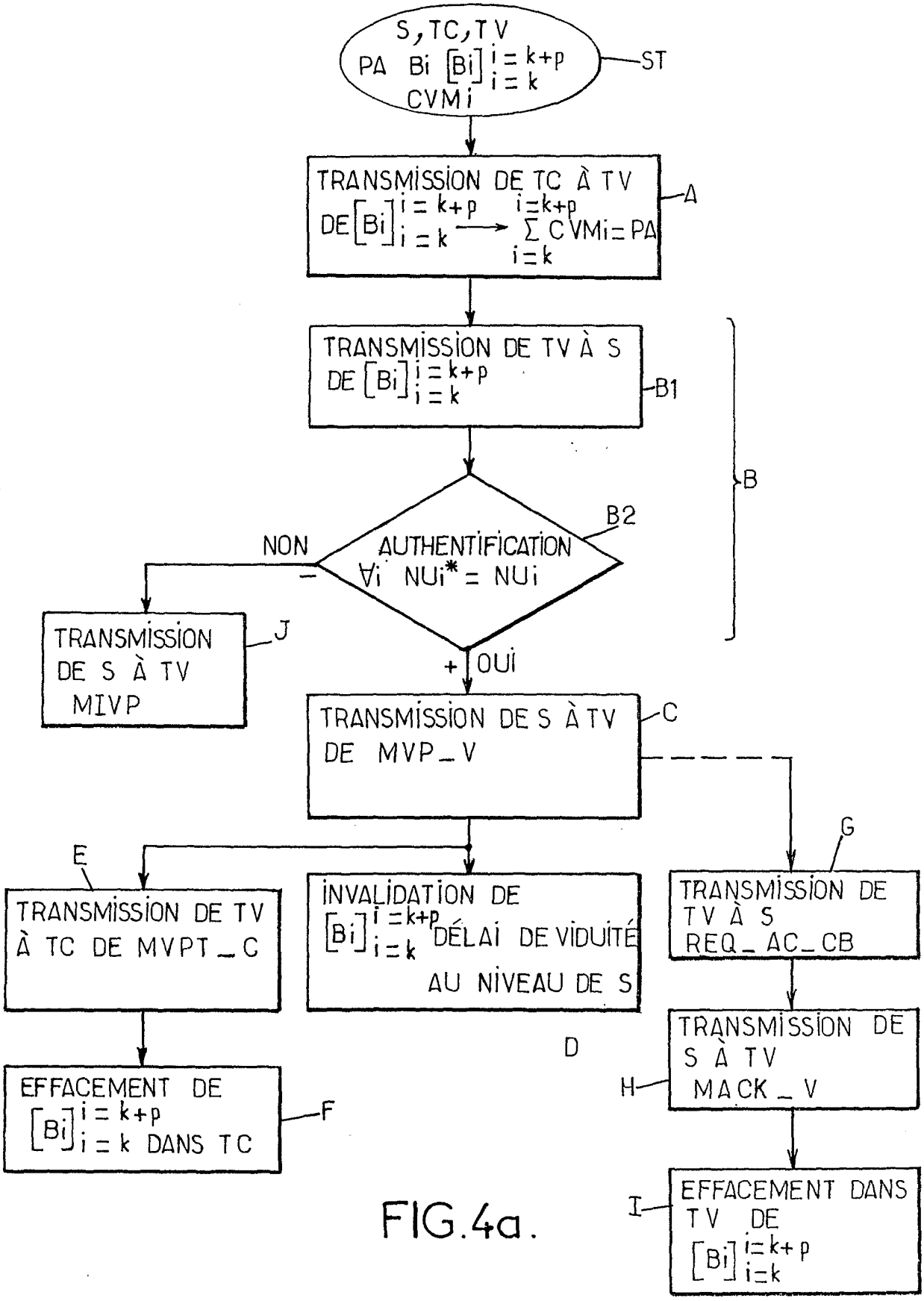

S, TC, TV
PA Bi [Bi] i=k+p i=k
CVMi
ST
TRANSMISSION DE TC À TV
DE [Bi] i=k+p i=k → i=k+p Σ i=k CVMi = PA
A
TRANSMISSION DE TV À S
DE [Bi] i=k+p i=k
B1
B
AUTHENTIFICATION
∀i NUi* = NUi
B2
NON
OUI
TRANSMISSION DE S À TV MIVP
J
TRANSMISSION DE S À TV DE MVP_V
C
E
TRANSMISSION DE TV À TC DE MVPT_C
INVALIDATION DE [Bi] i=k+p i=k DÉLAI DE VIDUITÉ AU NIVEAU DE S
D
G
TRANSMISSION DE TV À S REQ_AC_CB
TRANSMISSION DE S À TV MACK_V
H
EFFACEMENT DE [Bi] i=k+p i=k DANS TC
F
EFFACEMENT DANS TV DE [Bi] i=k+p i=k
I

FIG.4a.

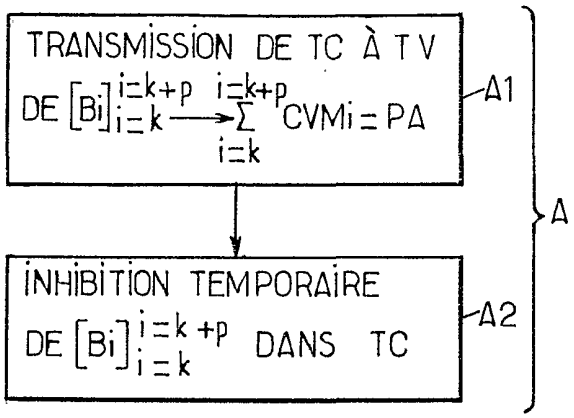


FIG.4b.

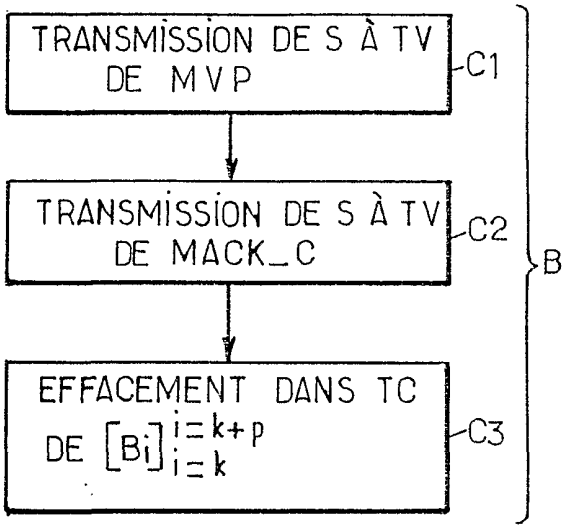


FIG.4c.

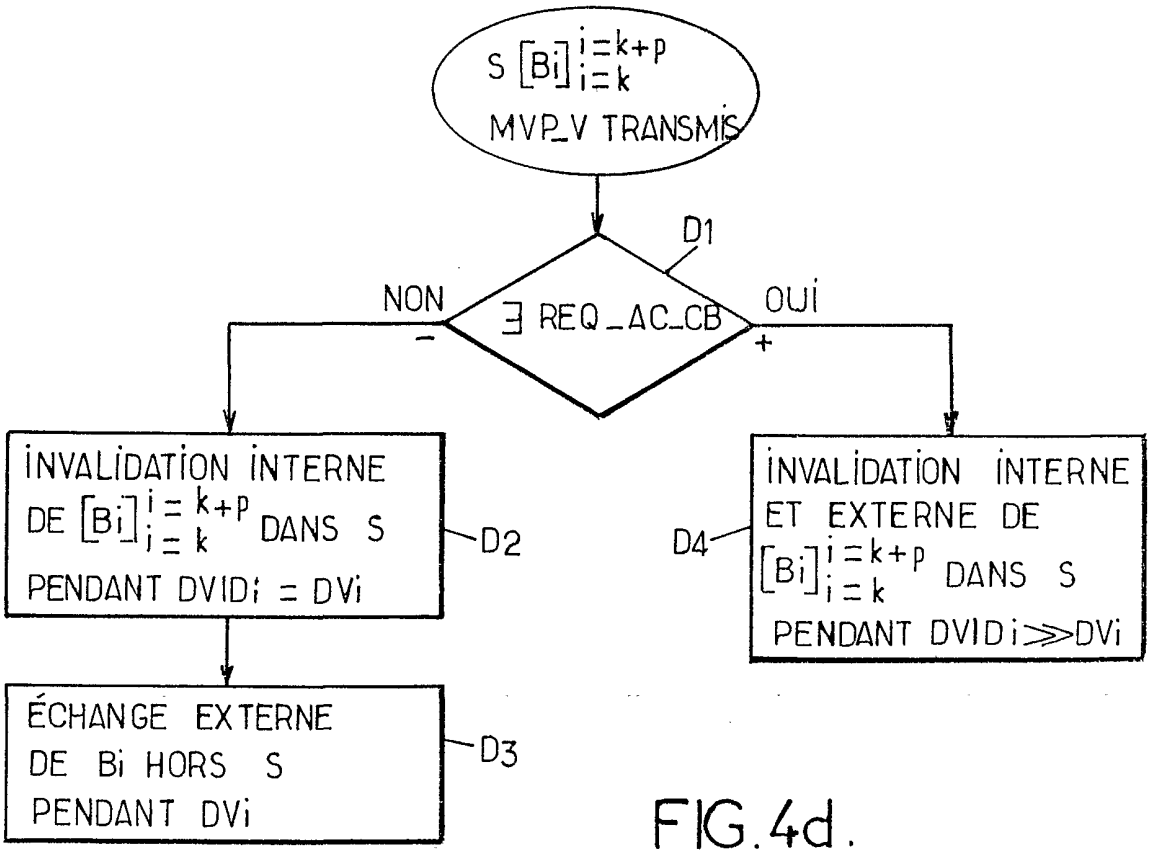


FIG.4d.

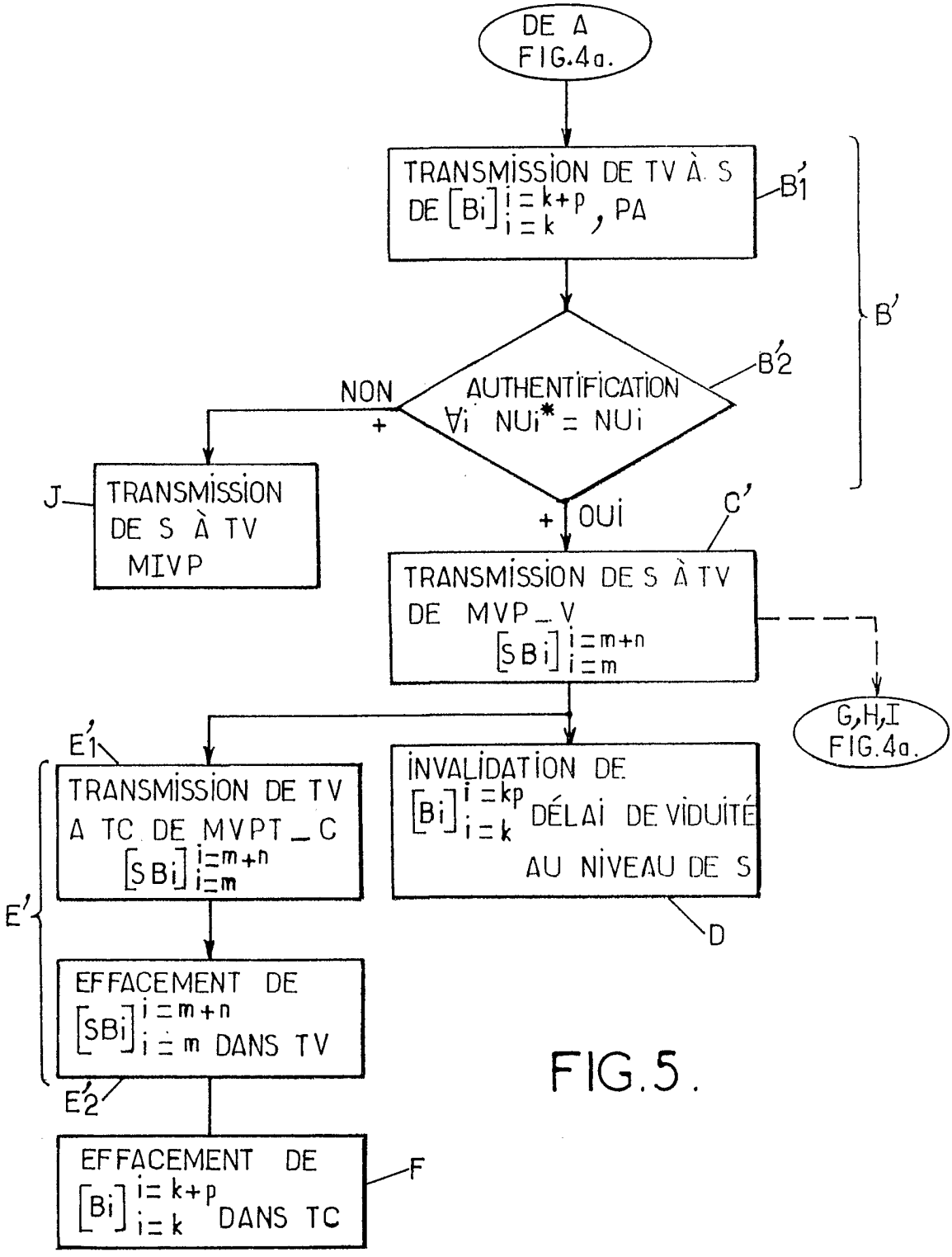

DE A FIG.4a.
TRANSMISSION DE TV À S DE [Bi] i=k+p i=k , PA
B'1
B'
AUTHENTIFICATION ∀i NUi* = NUi
B'2
NON
+
OUI
J
TRANSMISSION DE S À TV MIVP
C'
TRANSMISSION DE S À TV DE MVP_V [SBi] i=m+n i=m
G,H,I FIG.4a.
E'1
TRANSMISSION DE TV A TC DE MVPT_C [SBi] i=m+n i=m
INVALIDATION DE [Bi] i=kp i=k DÉLAI DE VIDUITÉ AU NIVEAU DE S
D
E'
EFFACEMENT DE [SBi] i=m+n i=m DANS TV
E'2
EFFACEMENT DE [Bi] i=k+p i=k DANS TC
F

FIG.5.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01912

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 22915 A (BRITISH TELECOMMUNICATIONS) 28 May 1998 (1998-05-28)	1
A	abstract; claims; figures page 7, line 19 -page 9, line 21	2,9,11, 13-16
Y	EP 0 574 990 A (PHILIPS PATENTVERWALTUNG) 22 December 1993 (1993-12-22) abstract; claims; figure 3 page 5, line 56 -page 6, line 41	1
A	WO 98 43211 A (BRITISH TELECOMMUNICATIONS) 1 October 1998 (1998-10-01) abstract; claims; figures page 6, line 30 -page 9, line 30	1,2,5, 7-11, 13-19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 October 2001	17/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01912

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 788 066 A (CITIBANK) 6 August 1997 (1997-08-06) abstract; claims; figures page 11, line 45 -page 15, line 11	1,5-11, 13-19
A	US 5 872 844 A (Y. YACOBI) 16 February 1999 (1999-02-16) abstract; claims; figures column 6, line 1 -column 8, line 55	1-3,5-16
A	FR 2 605 429 A (GRAFEILLE J-M.) 22 April 1988 (1988-04-22) the whole document	1-4
A	EP 0 865 010 A (FRANCE TELECOM) 16 September 1998 (1998-09-16)	
A	GB 2 317 790 A (R. BILLINGSLEY) 1 April 1998 (1998-04-01)	
A	WO 98 44429 A (ULTIMUS) 8 October 1998 (1998-10-08)	
A	US 5 999 625 A (M. BELLARE) 7 December 1999 (1999-12-07)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/01912

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9822915 A	28-05-1998	AU 4957197 A	10-06-1998
		EP 0941524 A1	15-09-1999
		WO 9822915 A1	28-05-1998
		JP 2001504612 T	03-04-2001
		US 6236981 B1	22-05-2001
EP 0574990 A	22-12-1993	DE 4219739 A1	23-12-1993
		DE 59309320 D1	04-03-1999
		EP 0574990 A2	22-12-1993
		JP 6215208 A	05-08-1994
		US 5436971 A	25-07-1995
WO 9843211 A	01-10-1998	WO 9843211 A1	01-10-1998
		AU 6740198 A	20-10-1998
		EP 0972276 A1	19-01-2000
EP 0788066 A	06-08-1997	US 5453601 A	26-09-1995
		EP 0785515 A2	23-07-1997
		EP 0785516 A2	23-07-1997
		EP 0785517 A2	23-07-1997
		EP 0788066 A2	06-08-1997
		EP 0785518 A2	23-07-1997
		EP 0803827 A2	29-10-1997
		EP 0784282 A2	16-07-1997
		AT 165463 T	15-05-1998
		AU 679359 B2	26-06-1997
		AU 2013695 A	20-07-1995
		AU 673304 B2	31-10-1996
		AU 2013795 A	20-07-1995
		AU 679360 B2	26-06-1997
		AU 2013895 A	20-07-1995
		AU 673305 B2	31-10-1996
		AU 2013995 A	20-07-1995
		AU 658233 B2	06-04-1995
		AU 2739292 A	17-06-1993
		BR 9204413 A	18-05-1993
		CA 2080452 A1	16-05-1993
		CN 1073789 A	30-06-1993
		DE 69225197 D1	28-05-1998
		DE 69225197 T2	19-11-1998
		DE 542298 T1	16-12-1993
		DK 542298 T3	11-01-1999
		EP 0542298 A2	19-05-1993
		ES 2046156 T1	01-02-1994
		FI 933208 A	14-07-1993
		GR 93300107 T1	29-10-1993
		HK 1002117 A1	17-03-2000
		HU 65212 A2	02-05-1994
		IL 103397 A	18-06-1996
		IL 116370 A	05-04-1998
		IL 116371 A	04-01-1998
		JP 3027128 B2	27-03-2000
		JP 9245108 A	19-09-1997
		JP 11096267 A	09-04-1999
		JP 11096268 A	09-04-1999
		JP 11096269 A	09-04-1999
		JP 11096270 A	09-04-1999
		JP 11096271 A	09-04-1999

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/01912

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0788066 A		JP 11096272 A	09-04-1999
		JP 11096273 A	09-04-1999
		JP 11096274 A	09-04-1999
		JP 6162059 A	10-06-1994
		JP 71117 B	
US 5872844 A	16-02-1999	NONE	
FR 2605429 A	22-04-1988	FR 2528197 A1	09-12-1983
		FR 2605429 A2	22-04-1988
		FR 2605429 B1	04-09-1992
		AT 34859 T	15-06-1988
		CA 1231449 A1	12-01-1988
		DE 3376899 D1	07-07-1988
		EP 0097110 A2	28-12-1983
		ES 523354 D0	16-08-1984
		ES 8407226 A1	16-11-1984
		JP 59052358 A	26-03-1984
		US 4774513 A	27-09-1988
EP 0865010 A	16-09-1998	FR 2760876 A1	18-09-1998
		EP 0865010 A1	16-09-1998
GB 2317790 A	01-04-1998	AU 4216597 A	17-04-1998
		WO 9813795 A1	02-04-1998
WO 9844429 A	08-10-1998	AU 6744598 A	22-10-1998
		CN 1259215 T	05-07-2000
		EP 1021800 A1	26-07-2000
		WO 9844429 A1	08-10-1998
		US 6119946 A	19-09-2000
US 5999625 A	07-12-1999	JP 10240848 A	11-09-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01912

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00 G06F17/60

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y A	WO 98 22915 A (BRITISH TELECOMMUNICATIONS) 28 mai 1998 (1998-05-28) abrégé; revendications; figures page 7, ligne 19 -page 9, ligne 21	1 2,9,11, 13-16
Y	EP 0 574 990 A (PHILIPS PATENTVERWALTUNG) 22 décembre 1993 (1993-12-22) abrégé; revendications; figure 3 page 5, ligne 56 -page 6, ligne 41	1
A	WO 98 43211 A (BRITISH TELECOMMUNICATIONS) 1 octobre 1998 (1998-10-01) abrégé; revendications; figures page 6, ligne 30 -page 9, ligne 30	1,2,5, 7-11, 13-19

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 octobre 2001	17/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 01/01912

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 788 066 A (CITIBANK) 6 août 1997 (1997-08-06) abrégé; revendications; figures page 11, ligne 45 -page 15, ligne 11	1,5-11, 13-19
A	US 5 872 844 A (Y. YACOBI) 16 février 1999 (1999-02-16) abrégé; revendications; figures colonne 6, ligne 1 -colonne 8, ligne 55	1-3,5-16
A	FR 2 605 429 A (GRAFEILLE J-M.) 22 avril 1988 (1988-04-22) le document en entier	1-4
A	EP 0 865 010 A (FRANCE TELECOM) 16 septembre 1998 (1998-09-16)	
A	GB 2 317 790 A (R. BILLINGSLEY) 1 avril 1998 (1998-04-01)	
A	WO 98 44429 A (ULTIMUS) 8 octobre 1998 (1998-10-08)	
A	US 5 999 625 A (M. BELLARE) 7 décembre 1999 (1999-12-07)	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/01912

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9822915	A	28-05-1998	AU	4957197 A	10-06-1998
			EP	0941524 A1	15-09-1999
			WO	9822915 A1	28-05-1998
			JP	2001504612 T	03-04-2001
			US	6236981 B1	22-05-2001
EP 0574990	A	22-12-1993	DE	4219739 A1	23-12-1993
			DE	59309320 D1	04-03-1999
			EP	0574990 A2	22-12-1993
			JP	6215208 A	05-08-1994
			US	5436971 A	25-07-1995
WO 9843211	A	01-10-1998	WO	9843211 A1	01-10-1998
			AU	6740198 A	20-10-1998
			EP	0972276 A1	19-01-2000
EP 0788066	A	06-08-1997	US	5453601 A	26-09-1995
			EP	0785515 A2	23-07-1997
			EP	0785516 A2	23-07-1997
			EP	0785517 A2	23-07-1997
			EP	0788066 A2	06-08-1997
			EP	0785518 A2	23-07-1997
			EP	0803827 A2	29-10-1997
			EP	0784282 A2	16-07-1997
			AT	165463 T	15-05-1998
			AU	679359 B2	26-06-1997
			AU	2013695 A	20-07-1995
			AU	673304 B2	31-10-1996
			AU	2013795 A	20-07-1995
			AU	679360 B2	26-06-1997
			AU	2013895 A	20-07-1995
			AU	673305 B2	31-10-1996
			AU	2013995 A	20-07-1995
			AU	658233 B2	06-04-1995
			AU	2739292 A	17-06-1993
			BR	9204413 A	18-05-1993
			CA	2080452 A1	16-05-1993
			CN	1073789 A	30-06-1993
			DE	69225197 D1	28-05-1998
			DE	69225197 T2	19-11-1998
			DE	542298 T1	16-12-1993
			DK	542298 T3	11-01-1999
			EP	0542298 A2	19-05-1993
			ES	2046156 T1	01-02-1994
			FI	933208 A	14-07-1993
			GR	93300107 T1	29-10-1993
			HK	1002117 A1	17-03-2000
			HU	65212 A2	02-05-1994
			IL	103397 A	18-06-1996
			IL	116370 A	05-04-1998
			IL	116371 A	04-01-1998
			JP	3027128 B2	27-03-2000
			JP	9245108 A	19-09-1997
			JP	11096267 A	09-04-1999
			JP	11096268 A	09-04-1999
			JP	11096269 A	09-04-1999
			JP	11096270 A	09-04-1999
			JP	11096271 A	09-04-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/01912

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0788066 A		JP 11096272 A	09-04-1999
		JP 11096273 A	09-04-1999
		JP 11096274 A	09-04-1999
		JP 6162059 A	10-06-1994
		JP 71117 B	
US 5872844 A	16-02-1999	AUCUN	
FR 2605429 A	22-04-1988	FR 2528197 A1	09-12-1983
		FR 2605429 A2	22-04-1988
		FR 2605429 B1	04-09-1992
		AT 34859 T	15-06-1988
		CA 1231449 A1	12-01-1988
		DE 3376899 D1	07-07-1988
		EP 0097110 A2	28-12-1983
		ES 523354 D0	16-08-1984
		ES 8407226 A1	16-11-1984
		JP 59052358 A	26-03-1984
		US 4774513 A	27-09-1988
EP 0865010 A	16-09-1998	FR 2760876 A1	18-09-1998
		EP 0865010 A1	16-09-1998
GB 2317790 A	01-04-1998	AU 4216597 A	17-04-1998
		WO 9813795 A1	02-04-1998
WO 9844429 A	08-10-1998	AU 6744598 A	22-10-1998
		CN 1259215 T	05-07-2000
		EP 1021800 A1	26-07-2000
		WO 9844429 A1	08-10-1998
		US 6119946 A	19-09-2000
US 5999625 A	07-12-1999	JP 10240848 A	11-09-1998